Express5800

NEC

ESMPRO/ServerAgent Ver. 4.5

ユーザーズガイド (Linux 編)

SA45_J-UG-L-010-01-003

目　次

本書で使う記号

本文中の記号

本書では3 種類の記号を使用しています。これらの記号は、次のような意味があります。

重要	ソフトウェアの操作などにおいて、守らなければならないことについて示しています。記載の手順に従わないときは、装置の故障、データの損失など、重大な不具合が起きるおそれがあります。
チェック	ソフトウェアの操作などにおいて、確認しておかなければならないことについて示しています。
ヒント	知っておくと役に立つ情報、便利なことについて示しています。

外来語のカタカナ表記

本書では外来語の長音表記に関して、国語審議会の報告を基に告示された内閣告示に原則準拠しています。但し、OS やアプリケーションソフトウェアなどの記述では準拠していないことがありますが、誤記ではありません。

商　標

ESMPRO は日本電気株式会社の登録商標です。
Linux は、Linus Torvalds 氏の日本およびその他の国における商標または登録商標です。
Red Hat、Red Hat Enterprise Linux は、米国 Red Hat, Inc.の米国およびその他の国における商標または登録商標です。
VMware は、VMware, Inc.の米国およびその他の国における商標または登録商標です。

その他、記載の会社名および商品名は各社の商標または登録商標です。
なお、本文には登録商標や商標に(TM)、(R)マークは記載しておりません。

本書についての注意、補足

1. 本書の内容の一部または全部を無断転載することは禁じられています。
2. 本書の内容に関しては将来予告なしに変更することがあります。
3. 弊社の許可なく複製・改変などを行うことはできません。
4. 本書は内容について万全を期して作成いたしましたが、万一ご不審な点や誤り、記載もれなどお気づきのことがありましたら、お買い求めの販売店にご連絡ください。
5. 運用した結果の影響については、4 項にかかわらず責任を負いかねますのでご了承ください。
6. 本書の説明で用いられているサンプル値は、すべて架空のものです。

この説明書は、必要なときすぐに参照できるよう、お手元に置いておくようにしてください。

最新版

本書は作成日時点の情報をもとに作られており、画面イメージやメッセージ、手順などが**実際のものと異なるときがあります。**変更されているときは適宜読み替えてください。
また、ユーザーズガイドをはじめとするドキュメントは、次のウェブサイトから最新版をダウンロードできます。

http://www.express.nec.co.jp/linux/dload/esmpro/docs.html

ESMPRO/ServerAgent Ver. 4.5

1

製品概要

ESMPRO/ServerAgent の製品概要について説明します。

製品概要

ESMPRO/ServerManager、ESMPRO/ServerAgent は、サーバーシステムの安定稼動と、効率的なサーバーシステム運用を目的としたサーバー管理ソフトウェアです。サーバーリソースの構成情報・稼動状況を管理し、サーバー障害を検出してシステム管理者へ通報することにより、サーバー障害の防止、障害に対する迅速な対処を可能にします。

サーバー管理の重要性

分散化システムにおいては、サーバーの安定稼動は必要不可欠です。また、安定稼動を保証するためには、サーバー管理の負担を軽減する必要があります。

サーバーの安定稼動

お客様の分散システムの中核を担うサーバーの停止は、即、お客様の営業機会、利益の損失につながります。そのため、サーバーはつねに万全の状態で稼動している必要があります。万が一サーバーで障害が発生した場合は、できるだけ早く障害の発生を知り、原因の究明、対処する必要があります。障害の発生から復旧までの時間が短ければ短いほど、利益(コスト)の損失を最小限にとどめることができます。

サーバー管理の負担軽減

分散化システムにおけるサーバー管理は多くの労力を必要とします。とくに大規模な分散化システム、遠隔地にあるサーバーとなればなおさらです。サーバー管理の負担を軽減することは、すなわちコストダウン(お客様の利益)につながります。

Express5800 シリーズにおけるサーバー管理

では、Express5800 シリーズをご利用のお客様がサーバー管理を行うには、どうすればよいのでしょうか?

Express5800 シリーズでは、このニーズに応えるため、サーバー管理ソフトウェア

「ESMPRO/ServerManager、ESMPRO/ServerAgent」

を Express5800 シリーズ(一部機種を除く)に、標準で添付しています。

ESMPRO/ServerManager、ESMPRO/ServerAgent をご利用いただくことにより、お客様の Express5800 シリーズを容易に管理できるようになります。VMware ESX では、コンソールオペレーティングシステムが、仮想カーネル(VMkernel)にあるため、Linux 版と同等の機能を提供しています。

ただし、標準で添付している ESMPRO/ServerAgent では、VMware ESX Server や仮想マシン(ゲスト OS)を監視できません。

VMware ESX のホスト OS(VMkernel)を監視するためのサーバー管理ソフトウェア製品として、

「ESMPRO/ServerAgent for VMware」

仮想マシン(ゲスト OS)を監視するためのサーバー管理ソフトウェア製品として、

「ESMPRO/ServerAgent for Guest OS (Windows/Linux)」

Express5800 シリーズ以外の他社製サーバーを監視するためのサーバー管理ソフトウェア製品として、

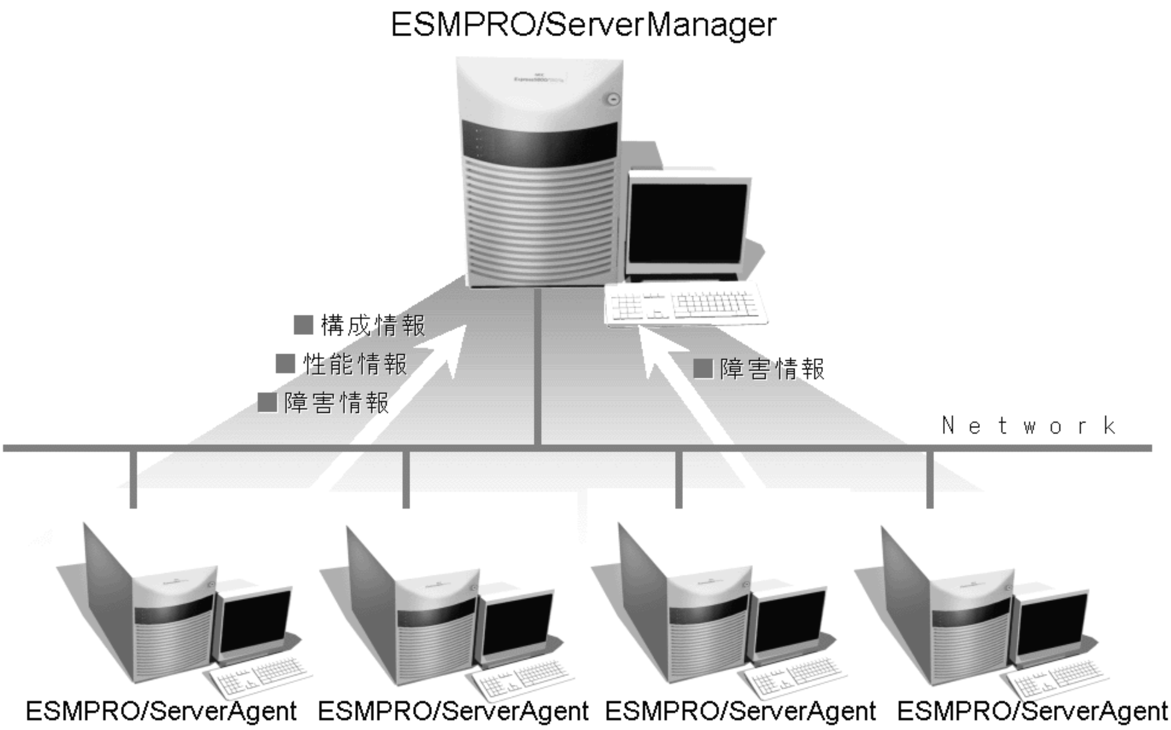
「他社機版 ESMPRO/ServerAgent (Windows/Linux)」

をご用意しておりますので、詳細は次のウェブサイトを参照してください。

http://www.nec.co.jp/pfsoft/smsa/index.html

ESMPRO/ServerManager、ESMPRO/ServerAgent とは?

ESMPRO/ServerManager、ESMPRO/ServerAgent は、ネットワーク上の Express5800 シリーズを管理・監視するサーバー管理ソフトウェアです。本製品を導入することにより、サーバーの構成情報・性能情報・障害情報をリアルタイムに取得・管理・監視できるほか、アラート通報機能により障害の発生を即座に知ることができるようになります。



ESMPRO/ServerManager、ESMPRO/ServerAgent の利用効果

ESMPRO/ServerManager、ESMPRO/ServerAgent は、多様化・複雑化するシステム環境における様々なニーズに対して十分な効果を発揮します。

サーバー障害を検出

ESMPRO/ServerAgent は、Express5800 シリーズの様々な障害情報を収集し、異常を判定します。サーバーで異常を検出したとき、ESMPRO/ServerManager へアラート通報します。

サーバー障害を防止

ESMPRO/ServerAgent は、障害の予防対策として、事前に障害の発生を予測する予防保守機能をサポートしています。筐体内温度上昇や、ファイルシステムの空き容量、ハードディスクドライブ劣化などを事前に検出できます。

サーバー稼動状況を管理

ESMPRO/ServerAgent は、Express5800 シリーズの詳細なハードウェア構成情報、性能情報を取得できます。取得した情報は ESMPRO/ServerManager をとおして参照できます。

分散したサーバーを一括管理

ESMPRO/ServerManager は、ネットワーク上に分散したサーバーを効率よく管理できる GUI インタフェースを提供します。

詳細は、次のウェブサイトからダウンロードできる ESMPRO サーバ管理ガイドを参照してください。

http://www.nec.co.jp/pfsoft/smsa/index.html

ダウンロード ＞ ドキュメント ＞ESMPRO/ServerManager, ServerAgent Ver.4(Windows)

ESMPRO/ServerAgent Ver. 4.5

2 監視機能

ESMPRO/ServerAgent の監視機能について説明します。

1. 監視設定

2. 全般プロパティ

3. CPU 負荷監視

4. Syslog 監視

5. ストレージ監視

6. ファイルシステム監視

7. ネットワーク(LAN)監視

8. OS ストール監視

9. シャットダウン監視

10. 共有センサ

1. 監視設定

本章では ESMPRO/ServerAgent が提供する監視機能を説明します。各監視機能の設定は、コントロールパネル(ESMagntconf)で変更します。ご使用の環境(装置、および ESMPRO/ServerAgent パッケージのインストール状況)により、一部設定できない項目があります。

・共有センサーのない筐体や装置では「共有センサ」は表示されません。

・「Mylex」がコントロールパネルに表示されるときがありますが、監視できません。

チェック

テキストモード(runlevel 3)では日本語が正しく表示できません。そのため、コントロールパネルを日本語で表示させるためには、ネットワーク経由(ssh コマンドなど)で別の日本語端末からログインし、一時的に LANG 環境変数を日本語環境に変更してからコントロールパネルを起動してください。コントロールパネルを起動するコンソールの LANG 環境変数を、ja_JP.eucJP へ変更して、作業してください。

　# echo $LANG　　…　現在の LANG 環境変数を確認します。

　# export LANG=ja_JP.eucJP

　# cd /opt/nec/esmpro_sa/bin/

　# ./ESMagntconf　(または)　./ESMpowersw

作業終了後に元の LANG 環境変数に変更してください。

※LANG 環境変数は、OS に合わせ、ja_JP.eucJP や ja_JP.UTF-8 を使用してください。

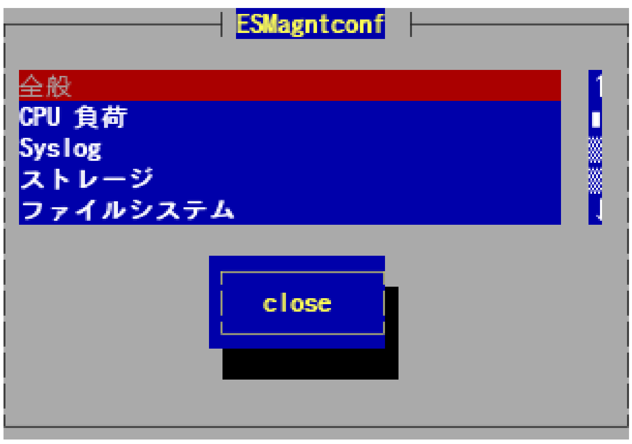
ヒント

コントロールパネルを複数のコンソールから起動しないでください。

後から実行したコンソールからは起動できず、『レジストリの読み込みに失敗しました。』と表示します。

コントロールパネル(ESMagntconf)の起動方法は以下のとおりです。

1. root 権限のあるユーザーでログインします。
2. ESMagntconf が格納されているディレクトリーに移動します。
   # cd /opt/nec/esmpro_sa/bin/
3. コントロールパネル(ESMagntconf)を起動します。
   # ./ESMagntconf



コントロールパネル(ESMagntconf)のメイン画面

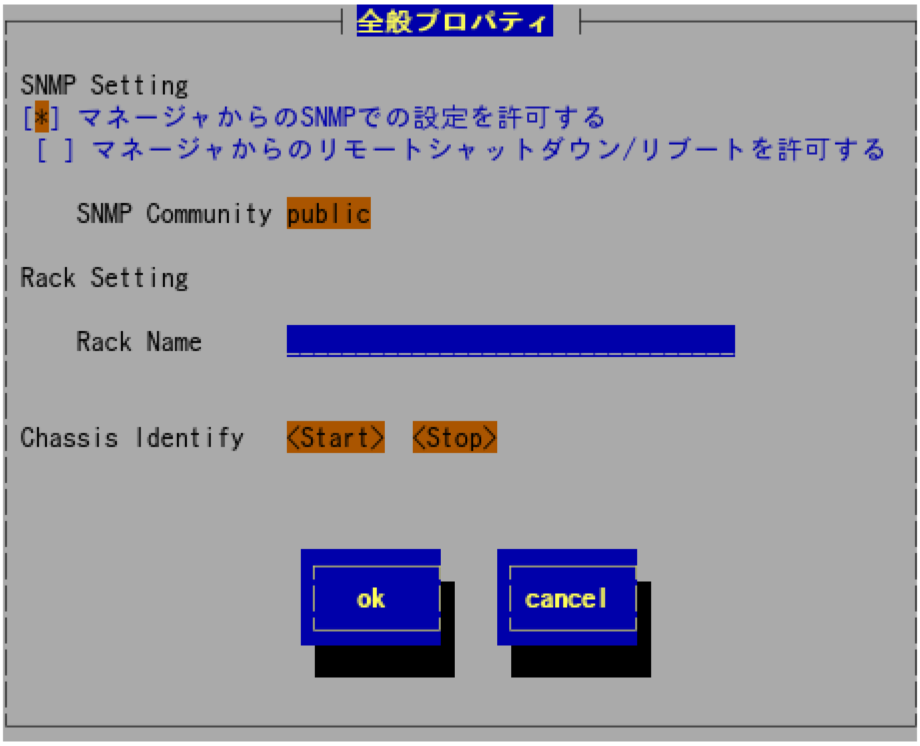
2. 全般プロパティ

機　能

ESMPRO/ServerManager から SNMP を利用した設定やシャットダウン／リブート、使用するコミュニティー名の設定、ラックマウント機種でのラック名の登録、筐体識別機能が使用できます。

設　定

コントロールパネル(ESMagntconf)の「全般」を選択して表示される[全般プロパティ]画面にて、設定ができます。



マネージャからの SNMP での設定を許可する

ESMPRO/ServerManager からの本機のしきい値変更等の動作設定の更新を許可するか､許可しないかを<スペース>キーで設定できます。許可するときは、チェックボックスをチェックします。

マネージャからのリモートシャットダウン/リブートを許可する

ESMPRO/ServerManager から本機をリモートシャットダウンまたはリモートリブートすることを許可するか、許可しないかを<スペース>キーで設定できます。許可するときは、チェックボックスをチェックします。「マネージャからの SNMP での設定を許可する」が許可されていないと「マネージャからのリモートシャットダウン/リブートを許可する」の許可はできません。

SNMP Community

ESMPRO/ServerAgent がローカルマシンの情報を取得するときや SNMP トラップを送信するときに使用する SNMP コミュニティー名を選択します。リストに表示されるコミュニティー名は、SNMP 環境設定ファイル(/etc/snmp/snmpd.conf)に登録されているコミュニティー名です。localhost に対して「READ WRITE」以上の権限を与えているコミュニティー名を<↑>か<↓>キーで選択してください。

Rack Name

本機がラックマウントタイプのとき、ラック名を設定できます。ラック名を設定することによりラック単位で管理できます。ラック名の最大長は、63 文字で、A～Z と a～z の英字、0～9 の数字、'.'、'_'、'-' のみ使用可能です。EM カード搭載装置のとき、EM カードから値を取得している為、本設定では値を設定できません。参照のみとなります。

> EM カード搭載のブレード収納ユニットに取り付けた CPU ブレードのときは、[全般プロパティ]画面から「Rack Name」を変更することはできません。Web コンソール機能等の EM カードの機能を使用して、設定してください。設定手順は、ブレード収納ユニットユーザーズガイドを参照してください。

Chassis Identify(筐体識別)

[start]ボタンを押すと筐体識別の機能(ID ランプ点滅または点灯)が作動し、[stop]ボタンを押すと筐体識別の機能が停止します。

[ok]ボタン

設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

3. CPU負荷監視

機　能

CPU 負荷監視機能は､CPU の高負荷状態を検出すると､syslog へ検出情報の記録と ESMPRO/ServerManager へ通報(アラート通報)します。ESMPRO/ServerManager を参照すると、異常や警告状態の CPU を確認できます。CPU の負荷状態は、“個々の CPU”と“CPU トータル”の 2 種類の単位で監視できます。そのため、個々の CPU にとらわれず、サーバー1 台を 1 つのパッケージとして監視できます。

既定値では CPU の負荷率は、監視しません。CPU 負荷率を監視するときは設定を変更します。CPU 負荷率のしきい値は、基本的に変更する必要ありません。任意の値に設定を変更することもできますが、変更されたしきい値によっては頻繁に CPU 負荷に関するアラートが通報されることも考えられます。CPU 負荷率のしきい値を変更するとき、システムの負荷によってアラートが頻繁に通報されないように、しきい値を設定してください。

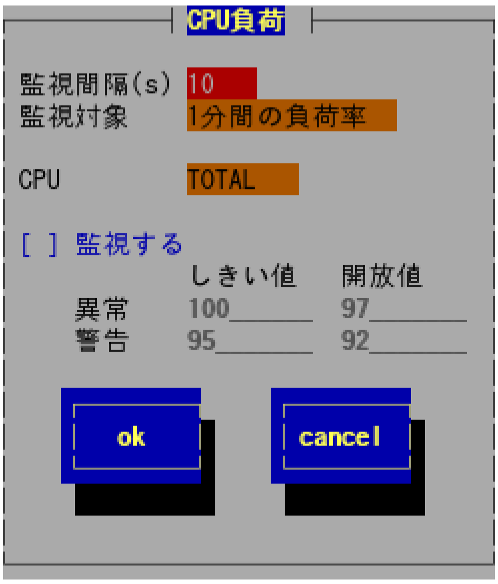
CPU 負荷率を監視するときの既定値は以下のとおりです。

監視間隔：10 秒
監視対象：1 分間の負荷率

監視間隔である 10 秒毎にその時点での使用率を取得し、監視対象である 1 分間の平均値[6(回)=60(対象秒)/10(間隔秒)]を「現在の使用率」として、しきい値と比較します。「現在の使用率」としきい値の比較は、ESMPRO/ServerAgent で設定した監視間隔である 10 秒毎に行ない、状態(正常/警告/異常)に変化があったときは通報します。監視対象を"1 分間の負荷率"から"5 分間の負荷率"に変更した場合は、監視対象である 1 分間の平均値[30(回)=300(対象秒)/10(間隔秒)]を「現在の使用率」とし、しきい値と比較します。

設　定

コントロールパネル(ESMagntconf)の「CPU 負荷」を選択して表示される[CPU 負荷]画面にて、CPU 負荷監視機能の「監視間隔」と「監視対象」、「しきい値」が設定できます。



監視間隔

CPU 負荷率のデータを採取する間隔(秒)が設定できます。
1、2、3、4、5、6、10、12、15、20、30、60 のいずれかの監視間隔を<↑>か<↓>キーで選択できます。
既定値は 10 秒です。

監視対象

監視の対象とする負荷率の種類が指定できます。
1 分間、5 分間、30 分間、1 時間、1 日間、1 週間の負荷率を<↑>か<↓>キーで選択できます。
既定値は「1 分間の負荷率」です。

CPU

監視設定の参照または設定する CPU を<↑>か<↓>キーで選択できます。

監視する

選択している CPU の負荷率監視の有効(チェックあり)と無効(チェックなし)を<スペース>キーで設定します。このチェックボックスをチェックしているときに「しきい値」と「開放値」を設定できます。
既定値は「監視しない」です。

しきい値 / 開放値

異常と警告の「しきい値」と「開放値」が設定できます。
0 から 100 の整数値で、次の大小関係を満たす必要があります。
100 ≧ しきい値(異常) ＞ 開放値(異常回復) ＞ しきい値(警告) ＞ 開放値(警告回復) ≧ 0
既定値は次のとおりです。

監視項目名	しきい値(異常)	開放値(異常回復)	しきい値(警告)	開放値(警告回復)
CPU 負荷率(%)	100	97	95	92

[ok]ボタン

設定した情報を登録し、この画面を閉じます。設定の変更は、次の監視間隔で有効になります。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

4. Syslog監視

機 能

Syslog 監視機能は設定されたキーワードが syslog に記録されると、ESMPRO/ServerManager へ通報(アラート通報)します。監視対象となる syslog は、"/var/log/messages"となり変更はできません。
また、監視対象となる syslog ローテート後のファイル名は、/etc/logrotate.conf に"dateext"が
　定義されていない : /var/log/messages.n [n=1, 2, 3, ...]
　定義されている　 : /var/log/messages-YYYYMMDD [YYYY=西暦年, MM=月, DD=日]
であり、他の命名規則となっているとき、Syslog 監視機能では、監視できません。
また、/etc/logrotate.d/syslog に"compress"(圧縮する)が定義されているとき、ローテート後のファイルはテキストではないため、Syslog 監視機能では、監視できません。
Red Hat Enterprise Linux 6 では、既定値で"dateext"が定義されています。
SUSE Linux Enterprise Server では、既定値で"compress"が定義されています。

"/var/log/messages" の文字列を含まないファイルを監視対象として、1 つ追加できます。既定監視対象をチェックした後、追加監視対象のファイルをチェックするため、監視間隔のタイミングにより、時系列が逆転するときがあります。追加することのできる監視対象は、syslog と同じ以下のフォーマットで出力されるファイルのみとなり、監視対象ファイルの一行目は監視しません。

　　%b %d %H:%M:%S %HOSTNAME% %MESSAGE%
　　　%b　ロケールによる省略形の月の名前 (Jan～Dec),　　%d　日(月内通算日数 2 桁) (1～31)
　　　%H　時 (00～23),　　%M　分 (00～59),　　%S　秒 (00～59)
　　　%HOSTNAME%　ホスト名,　　%MESSAGE%　メッセージ (通報内容)

ログローテートするファイルを指定した場合は、ログのファイル名の切り替わるタイミングで、追加監視対象ファイル後半の一部が監視できないときがあります。VMware ESX で記録される/var/log/vmkernel を指定した場合は、ログローテート後のファイル名[vmkernel.1, vmkernel.2 ...]をサポートします。

"/var/log/messages"の文字列を含まないファイルを監視対象として、1 つ追加できます。既定監視対象と追加監視対象をチェックした後、ファイル監視対象のファイルをチェックするため、監視間隔のタイミングにより、時系列が逆転するときがあります。また、ログローテート後のファイル名については、サポートしておりませんので、ログのファイル名の切り替わるタイミングで、ファイル監視対象のファイル後半の一部が監視できないときがあります。追加することのできる監視対象のファイルフォーマットに指定はありません。

Syslog イベントは、ESMPRO/ServerAgent インストール時にあらかじめ登録している Syslog イベント以外に、システム環境に応じた新たなソース、イベントを追加/削除できます。Syslog イベントの追加/削除方法は、本書の 3 章(5. Syslog イベントの設定)を参照してください。

設 定

コントロールパネル(ESMagntconf)の「Syslog」を選択して表示される[Syslog]画面にて、Syslog 監視の「監視間隔」、「既定監視対象」「追加監視対象」が表示され、「追加監視対象」にて"/var/log/messages"の文字列を含まないファイルを監視対象に設定できます。



監視間隔(s)

Syslog 監視機能の監視する間隔(秒)が設定できます。
既定値は 300 秒です。
設定可能範囲は 10〜3600 秒です。

既定監視対象

"/var/log/messages "からの変更、削除はできません。

追加監視対象

"/var/log/messages"の文字列を含まないファイルを監視対象として、パスの長さが 255 バイト以下となる絶対パスで設定できます。相対パスでの設定はできません。
既定値は空白で、追加監視対象は設定されていません。

ファイル監視対象

"/var/log/messages"の文字列を含まないファイルを監視対象として、パスの長さが 255 バイト以下となる絶対パスで設定できます。相対パスでの設定はできません。
既定値は空白で、ファイル監視対象は設定されていません。

[ok]ボタン

設定した情報を登録し、この画面を閉じます。設定の変更は、次の監視間隔で有効になります。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

5. ストレージ監視

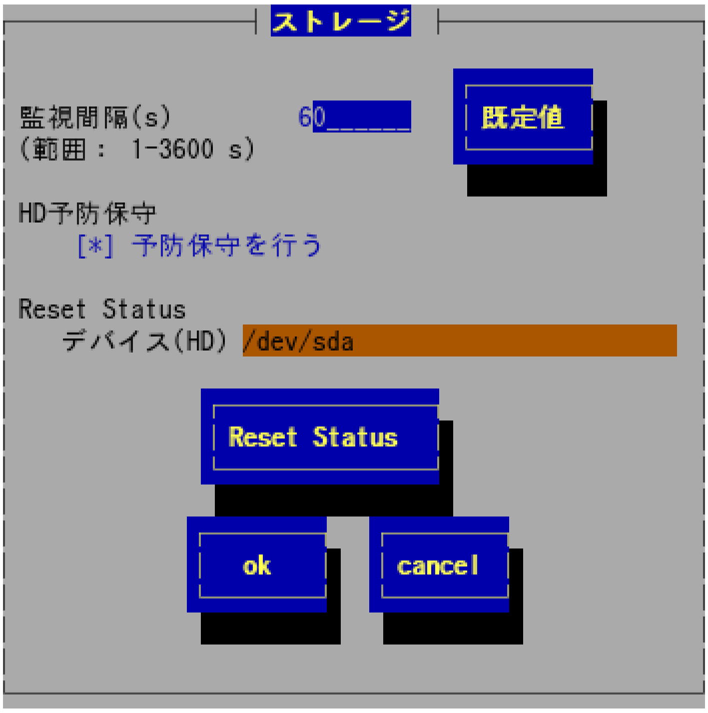
機 能

ストレージ監視機能は、ハードディスクドライブの S.M.A.R.T.機能(Self-Monitoring, Analysis and Reporting Technology)を使用して、ハードディスクドライブのエラーを検出すると、syslog へ検出情報の記録と ESMPRO/ServerManager へ通報(アラート通報)します。監視対象は、ハードディスクドライブ単体構成のみであり、RAID 構成や FC、USB などのストレージデバイスは、監視しません。そのため、ストレージ構成に応じた管理ソフトウェアを導入してください。

S.M.A.R.T.機能とは、故障に関するデータを各ハードディスクドライブが内部で管理し、近い将来故障すると判断したときはハードディスクドライブ自身がエラーを通知する機能です。各ハードディスクドライブベンダーは、自社製ハードディスクドライブに適したしきい値を予防保守判定に使用しています。

設 定

コントロールパネル(ESMagntconf)の「ストレージ」を選択して表示される[ストレージ]画面にて、ストレージ監視機能の「監視間隔」などの監視設定、ハードディスクドライブ管理情報のリセットができます。



監視間隔

監視する間隔(秒)が設定できます。
既定値は 60 秒です。
設定可能範囲は 1～3600 秒です。

[既定値]ボタン

ボタンを押すと、既定値が設定されます。

予防保守を行う

ハードディスクドライブ予防保守機能の有効(チェックあり)と無効(チェックなし)を<スペース>キーで設定します。

既定値は”有効”です。

ハードディスクドライブ予防保守機能を無効、もしくは、有効にすると、設定した監視対象すべてのハードディスクドライブに対して、変更した内容が設定されます。個々のハードディスクドライブに対して、有効や無効は、設定できません。

Reset Status デバイス(HD)

設定対象のディスクを<↑>か<↓>キーで選択できます。

[Reset Status]ボタン

ストレージ監視機能が独自に管理している監視対象ディスクの情報をリセットします。

リセットするのは本機能が独自に管理している情報であり、監視対象ディスクに対しては書き込みしません。

> チェック
>
> ストレージ監視機能は予防保守するため、ハードディスクドライブの状態を独自に管理しています。そのため、ハードディスクドライブを交換したときは、管理情報を手動でリセットします。

[ok]ボタン

設定した情報を登録し、この画面を閉じます。設定の変更は、次の監視間隔で有効になります。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

6. ファイルシステム監視

機 能

ファイルシステム監視機能は、OS にマウントされているファイルシステムの空き容量不足を検出すると、syslog へ検出情報の記録と ESMPRO/ServerManager へ通報(アラート通報)します。
ESMPRO/ServerManager を参照すると、空き容量の不足したマウントポイントを確認できます。

ファイルシステム監視機能は、以下の条件をすべて満たすとき監視対象となります。

・ファイルシステムのデバイスタイプ※1 が以下のとき
  ide, rd, sd, sr, md, ramdisk, dac960, DAC960, device-mapper, dd
  ※1 デバイスタイプは、マウントポイント(/etc/mtab)を確認し、ディスク I/O 情報(/proc/diskstats)と、ブロックデバイス(/proc/devices)から判断します。
  以下の例では、sda1 と sda2 のデバイスタイプは、"sd"です。

```
[/etc/mtab 抜粋]
  /dev/sda1 /boot ext3 rw 0 0
  /dev/sda2 / ext3 rw 0 0
[/proc/diskstats 抜粋]
     8      1 sda1 127 984 13844 331 6 1 14 496 0 770 827
     8      2 sda2 24361 15137 1112602 115034 10027 25261 282312 195758 0 47660 310799
[/proc/devices 抜粋]
  Block devices:
    1 ramdisk
    8 sd
```

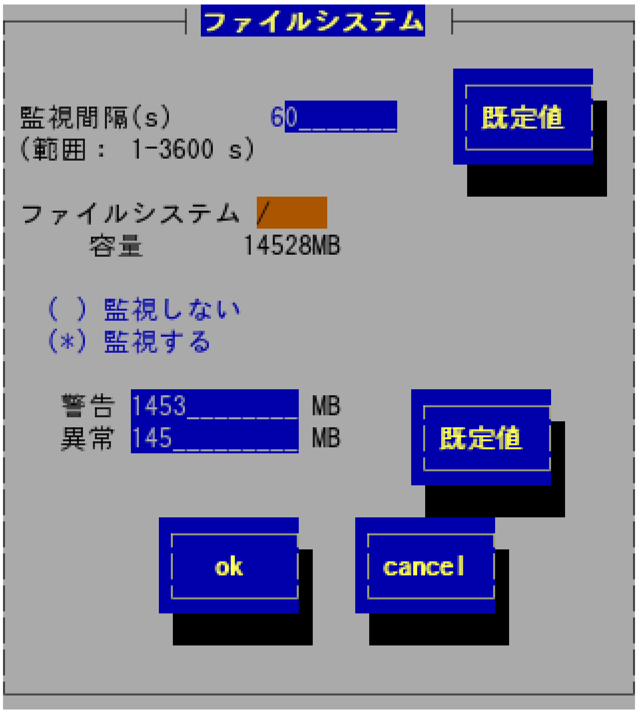
・ファイルシステムのタイプ(/etc/mtab 内に記載)が以下のとき
  affs, coda, ext, ext2, ext3, ext4, hfs, hpfs, jfs, minix, msdos, ntfs, reiserfs, sysv, ufs, umsdos, vfat, xfs, xiafs

  以下のファイルシステムの動作は検証済みです。
    ext2, ext3, ext4, jfs, minix, msdos, ntfs, reiserfs, vfat, xfs
  以下のファイルシステムの動作は未検証です。
  サポートしているカーネルが古いファイルシステムも含まれており、過去のバージョンでは動作を検証済みであるため、論理的には監視対象となります。
    affs, coda, ext, hfs, hpfs, sysv, ufs, umsdos, xiafs

・ファイルシステムの容量が 100MB 以上のとき

設 定

コントロールパネル(ESMagntconf)の「ファイルシステム」を選択して表示される[ファイルシステム]画面にて、ファイルシステム監視機能の「監視間隔」などの監視設定ができます。



監視間隔(s)

監視する間隔(秒)が設定できます。
既定値は 60 秒です。
設定可能範囲は 1～3600 秒です。

[既定値]ボタン

ボタンを押すと、監視間隔の既定値が設定されます。

ファイルシステム

監視をするファイルシステムを<↑>か<↓>キーで選択できます。

監視しない

ファイルシステム監視をしないときは、<スペース>キーで選択してチェックします。
既定値は"監視する"です。

監視する

ファイルシステム監視をするときは、<スペース>キーで選択してチェックします。
このチェックボックスをチェックしている時のみ、警告と異常のしきい値を設定できます。
既定値は"監視する"です。

しきい値

「警告」と「異常」の「しきい値」が設定できます。
単位は MB で、次の大小関係を満たす必要があります。
　全容量 ＞ 警告 ＞ 異常 ＞ 0
「警告」の既定値は全容量の約 10%、「異常」の既定値は全容量の約 1%です。

[既定値]ボタン

ボタンを押すと、しきい値の既定値が設定されます。

[ok]ボタン

設定した情報を登録し、この画面を閉じます。設定の変更は、次の監視間隔で有効になります。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

7. ネットワーク(LAN)監視

機 能

ネットワーク(LAN)監視機能は、監視間隔中に発生した破棄パケットやエラーパケットが設定されたしきい値を超えたとき syslog へ検出情報の記録と ESMPRO/ServerManager へ通報(アラート通報)します。異常を検出したあと、すぐに回復しているときは問題ありませんが、回復しなかったときや異常が頻繁に発生するときは、ネットワーク環境(ハードウェアも含め)の確認や、ネットワークの負荷を分散してください。

ネットワーク(LAN)監視機能は、監視間隔中に発生した送受信パケット数に対する割合で判断しているので、一時的なネットワーク負荷により検出するときがあります。そのため、LAN の障害の監視としては確実性が高いとは言えないことから、ESMPRO/ServerAgent Ver.4.3 以降では、監視設定の既定値は無効としています。

■ネットワーク(LAN)監視を有効にするときは、ESMlan の設定を変更した後、ESMlan を起動します。

```
# /sbin/chkconfig --level 35 ESMlan on
# /etc/init.d/ESMlan start
```

■ネットワーク(LAN)監視設定を無効にするときは、ESMlan の設定を変更した後、ESMlan を停止します。

```
# /sbin/chkconfig ESMlan off
# /etc/init.d/ESMlan stop
```

設 定

コントロールパネル(ESMagntconf)の「LAN」を選択して表示される[LAN]画面にて、ネットワーク(LAN)監視機能の「監視間隔」と「しきい値」が設定できます。



監視間隔

監視する間隔(秒)が設定できます。
既定値は 180 秒です。
設定可能範囲は 1～3600 秒です。

回線障害発生の割合

監視周期あたりの送受信パケット中の回線障害に繋がるエラーが発生した割合の「しきい値」が設定できます。エラーを検出した時、ただちに通報させたいときは、0 を指定してください。
既定値は 50%です。

設定可能範囲は 0～100%です。
回線障害は、ネットワークケーブルが外れているときや HUB の電源が入っていない時などに発生します。

各エラーは、以下のような原因で発生します。

エラー	原因
アライメントエラー	サイズがオクテット(8)単位でない受信パケット
FCS エラー	チェックサムでエラーが出た受信パケット
キャリアなし	パケット送信時の回線確認でエラー

送信リトライ発生の割合

監視周期当たりの総送信パケット中のパケットの衝突、遅延で送信されたパケットの割合の「しきい値」が設定できます。送信リトライは、本機の送受信が高負荷状態の時などに発生します。
既定値は 35%です。
設定可能範囲は 10～50%です。

送信アボート発生の割合

監視周期当たりの総送信パケット中の超過衝突等により、破棄されたパケットの割合の「しきい値」が設定できます。送信アボートは、本機の送受信が高負荷状態の時などに発生します。
既定値は 35%です。
設定可能範囲は 10～50%です。

[ok]ボタン

設定した情報を登録し、この画面を閉じます。設定の変更は、次の監視間隔で有効になります。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

8. OSストール監視

機　能

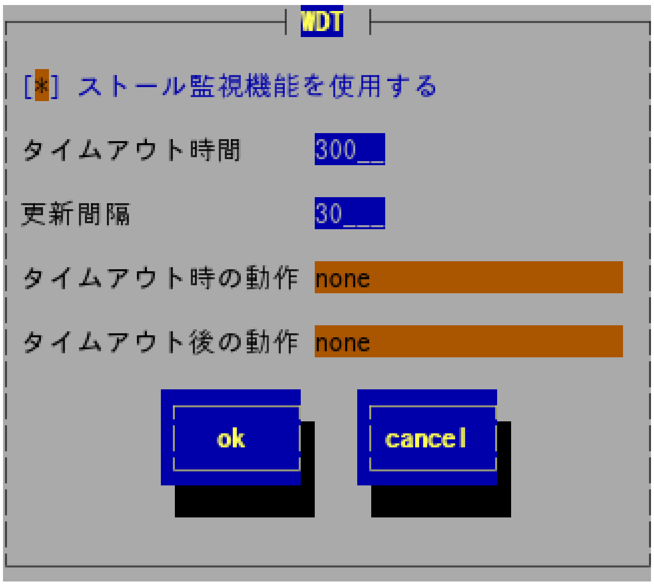
OS ストール監視機能は、ウォッチドックタイマー(ソフトウェアストール監視用タイマー)をサーバーマネージメントドライバーが定期的に更新することにより、OS の動作状況を監視します。ウォッチドックタイマーが更新されなくなると、タイマーがタイムアウトとなり、OS が停止している状態と判断して、「タイムアウト時の動作」に設定している動作をします。その後、「タイムアウト後の動作」に設定している動作をします。OS が停止している状態のため、ESMPRO/ServerAgent は、リアルタイムに動作できませんが、次回の OS 起動時にストールが発生したことを検出し、syslog へ検出情報の記録と ESMPRO/ServerManager へ通報(アラート通報)します。
コントロールパネル(ESMagntconf)からは、サーバーマネージメントドライバーが使用する設定を変更できます。

ヒント

lsmod コマンドで"mainte"が表示されているときは、サーバーマネージメントドライバーを利用して OS ストール監視をしています。"mainte"が表示されないときは、OpenIPMI を利用しています。OpenIPMI を利用した OS ストール監視の対象 OS、および設定手順は、本書の 4 章(4. OpenIPMI を利用した OS ストール監視)を参照してください。

設　定

コントロールパネル(ESMagntconf)の「WDT」を選択して表示される[WDT]画面にて、OS ストール監視機能の「タイムアウト時間」などの監視設定が設定できます。これにより、OS ストールが発生したときの復旧方法が設定できます。



ストール監視機能を使用する

OS ストール監視機能の有効(チェックあり)と無効(チェックなし)が<スペース>キーで設定できます。
既定値は「有効」です。

タイムアウト時間

OS がストールしたと判定する時間を秒単位で設定できます。
既定値は以下のとおりです。
300 秒：Red Hat Enterprise Linux 5 以降
Asianux Server 3
180 秒：上記以外の OS
設定可能範囲は、90～600 秒です。

更新間隔

タイムアウト時間のタイマーを更新する間隔を秒数で設定できます。
既定値は 30 秒です。
設定可能範囲は 30～60 秒です。
たとえば、タイムアウト時間が 180 秒、更新間隔が 30 秒のとき、ストールが発生してから、ストールしたと判定する時間は、150 秒から 180 秒の間になります。

タイムアウト時の動作

タイムアウト時の動作を<↑>か<↓>キーで選択できます。

none	何もしません
NMI	NMI を発生させます。(VMware では NMI は発生しません。)

※NMI:Non-maskable Interrupt の略で、ハードウェアの優先度が高い割り込みです。
既定値は以下のとおりです。
none：Red Hat Enterprise Linux 5 以降
Asianux Server 3
NMI ：上記以外の OS

タイムアウト後の動作

タイムアウト後の復旧方法を<↑>か<↓>キーで選択できます。

none (既定値)	何もしません。
リセット	システムをリセットし再起動を試みます。
電源断	システムの電源を切断します。
パワーサイクル	いったん電源 OFF し、直後に再度電源 ON します。

既定値は「none」です。

[ok]ボタン

設定した情報を登録し、この画面を閉じます。設定の変更は、次の監視間隔で有効になります。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

9. シャットダウン監視

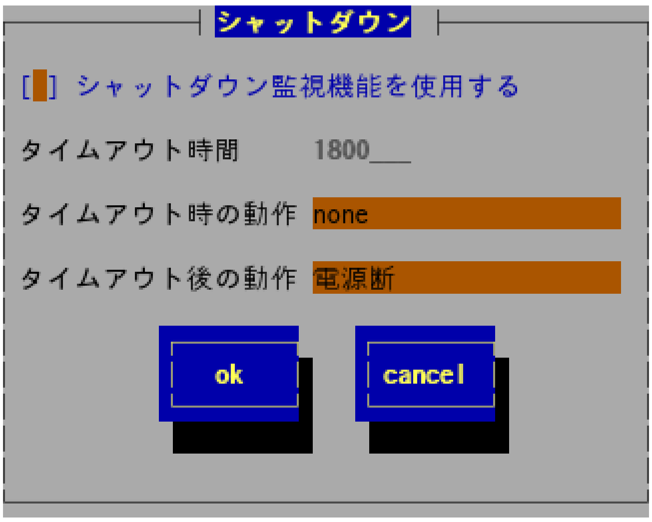
機 能

シャットダウン監視機能は、ウォッチドックタイマー(ソフトウェアストール監視用タイマー)をサーバーマネージメントドライバーが更新することにより、シャットダウン処理の開始から電源断までの時間を監視します。
ウォッチドックタイマーが更新されなくなると、タイマーがタイムアウトとなり、OS が停止している状態と判断して、「タイムアウト時の動作」に設定している動作をします。その後、「タイムアウト後の動作」に設定している動作をします。OS が停止している状態のため、ESMPRO/ServerAgent は、リアルタイムに動作できませんが、次回の OS 起動時にストールが発生したことを検出し、syslog へ検出情報の記録と ESMPRO/ServerManager へ通報(アラート通報)します。コントロールパネル(ESMagntconf)からは、サーバーマネージメントドライバーが使用する設定を変更できます。

> ヒント
>
> lsmod コマンドで“mainte”が表示されているときは、サーバーマネージメントドライバーを利用してシャットダウン監視をしています。“mainte”が表示されないときは、OpenIPMI を利用しています。OpenIPMI 方式では、シャットダウン時のウォッチドッグタイマーに任意の設定をすることができないため、本機能は、ESMPRO/ServerAgent では未サポートとなります。

設 定

コントロールパネル(ESMagntconf)の「シャットダウン」を選択して表示される[シャットダウン]画面にて、シャットダウン監視機能の「タイムアウト時間」などの監視設定が設定できます。これにより、シャットダウン処理中に OS ストールが発生したときの復旧方法が設定できます。



シャットダウン監視機能を使用する

シャットダウン監視する機能を有効(チェックあり)と無効(チェックなし)が<スペース>キーで設定できます。
既定値は「無効」です。

タイムアウト時間

シャットダウン処理中に OS がストールしたと判定する時間を秒単位で設定できます。

既定値は 1800 秒です。

設定可能範囲は 300～6000 秒です。

タイムアウト時の動作

タイムアウト時の動作を<↑>か<↓>キーで選択できます。

none (既定値)	何もしません。
NMI	NMI を発生させます。(VMware で NMI は発生しません。)

※NMI: Non-maskable Interrupt の略で、ハードウェアの優先度が高い割り込みです。

既定値は「none」です。

タイムアウト後の動作

タイムアウト後の復旧方法を<↑>か<↓>キーで選択できます。

none	何もしません。
リセット	システムをリセットし再起動を試みます。
電源断 (既定値)	システムの電源を切断します。
パワーサイクル	いったん電源 OFF し、直後に再度電源 ON します。

既定値は「電源断」です。

[ok]ボタン

設定した情報を登録し、この画面を閉じます。設定の変更は、次の監視間隔で有効になります。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

10. 共有センサ

機 能

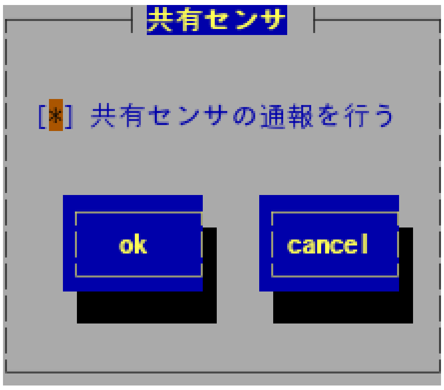
共有センサーに関する故障を検出すると、syslog へ検出情報の記録と ESMPRO/ServerManager へ通報(アラート通報)します。共有センサーが存在する同じ筐体内にて、複数の ESMPRO/ServerAgent が動作しているとき、故障を検出したすべての ESMPRO/ServerAgent から通報されますので、重複した通報となります。

本設定では、共有センサーに関する通報を抑止(停止)できます。すべての ESMPRO/ServerAgent からの通報を無効にすると、共有センサーに関する通報しませんので、すくなくとも､ひとつの ESMPRO/ServerAgent からの通報は、有効に設定してください。

Express5800/140Rf-4, R140a-4 はハードウェアとしては､共有センサーは存在しませんが､SDR(Sensor Data Record : ハードウェアセンサーのデータ)には、PowerSupply センサーの領域に共用センｅサーを示す情報があるため、共有センサーと判断し、コントロールパネルに[共有センサ]を表示します。設定を無効にしても通報を抑止せず、すべての ESMPRO/ServerAgent から通報します。

設 定

コントロールパネル(ESMagntconf)の「共有センサ」を選択して表示される[共有センサ]画面にて、共有センサーに関する通報の有効/無効が設定できます。



共有センサの通報を行う

共有センサの通報を有効(チェックあり)と無効(チェックなし)に<スペース>キーで設定できます。
既定値はチェックありで、“有効”です。

[ok]ボタン

設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

ESMPRO/ServerAgent Ver. 4.5

3 通報機能

ESMPRO/ServerAgent の通報機能について説明します。

1. 通報設定

2. 基本設定

3. 通報先リストの設定

4. エージェントイベントの設定

5. Syslog イベントの設定

1. 通報設定

本章では、どのようなイベントをどこの通報先にいつ通報するかといった通報設定の機能を説明しています。通報設定は、コントロールパネル(ESMamsadm)で設定します。

マネージャ通報には、次の 3 種類があります。

1. マネージャ通報(SNMP)
   ESMPRO/ServerAgent 独自に SNMP Trap(UDP トラップ)を送信します。ESMPRO/ServerManager 以外の「SNMP Trap 受信をサポートしているマネージャー」にも通報できます。

2. マネージャ通報(TCP_IP In-Band)
   TCP/IP を利用して、ESMPRO/ServerManager に通報するため、信頼性の高い通報をする場合に使用します。

3. マネージャ通報(TCP_IP Out-of-Band)
   TCP_IP In-Band と同様に TCP/IP を利用して、ESMPRO/ServerManager に通報しますが、PPP(Point to Point Protocol)を介して通報します。したがって、ESMPRO/ServerAgent と ESMPRO/ServerManager が遠隔地に存在し、公衆回線を通して、通報する場合(Wide Area Network 環境)に使用します。また、ダイヤルアップ接続となるため、ESMPRO/ServerAgent 側、ESMPRO/ServerManager 側のそれぞれにモデムと電話回線が必要となります。

チェック

テキストモード(runlevel 3)では、日本語が正しく表示できません。そのため、コントロールパネル(ESMamsadm)を日本語で表示させるためには、ネットワーク経由(ssh コマンドなど)で別の日本語端末からログインし、一時的に LANG 環境変数を日本語環境に変更してからコントロールパネル(ESMamsadm)を起動してください。コントロールパネル(ESMamsadm)を起動するコンソールの LANG 環境変数を「ja_JP.eucJP」へ変更して、作業してください。

```
# echo $LANG   …   現在の LANG 環境変数を確認します。
# export LANG=ja_JP.eucJP
# cd /opt/nec/esmpro_sa/bin/
# ./ESMamsadm
```

作業終了後に元の LANG 環境変数へ変更してください。

※LANG 環境変数は、OS に合わせ、ja_JP.eucJP や ja_JP.UTF-8 等を使用してください。

ヒント

コントロールパネルを複数のコンソールから起動しないでください。
後から実行したコンソールからは起動できず、『レジストリの読み込みに失敗しました。』と表示します。

コントロールパネル(ESMamsadm)の起動方法は以下のとおりです。

1. root 権限のあるユーザーでログインします。
2. ESMamsadm が格納されているディレクトリーに移動します。
   ```
   # cd /opt/nec/esmpro_sa/bin/
   ```
3. コントロールパネル(ESMamsadm)を起動します。
   ```
   # ./ESMamsadm
   ```



コントロールパネル(ESMamsadm)のメイン画面

■通報手段として SNMP による通報をするとき

ESMPRO/ServerAgent のインストール時にあらかじめ、監視イベントに対して SNMP 通報手段による通報設定がひととおり設定済みとなっています。通報基本設定にて、通報先となる ESMPRO/ServerManager が導入されているマシンの IP アドレスを設定するだけで、通報準備が整います。SNMP による通報をするときの設定につきましては、本書の 2 章(2.1.1. マネージャ通報(SNMP)の基本設定)を参照してください。

■通報手段として SNMP 以外による通報をするとき

以下の流れに従って設定してください。

1. 通報の基本設定をします。(通報基本設定)
   TCP_IP In-Band による通報をするときの基本設定は、本書の 2 章(2.1.2. マネージャ通報(TCP_IP In-Band)の基本設定)を参照してください。
   TCP_IP Out-of-Band による通報をするときの基本設定は、本書の 2 章(2.1.3. マネージャ通報(TCP_IP Out-of-Band)の基本設定)を参照してください。

2. 通報の宛先リストを設定します。(通報先リストの設定)
   TCP_IP In-Band による通報をするときの宛先設定は、本書の 2 章(3.1.1. 通報手段がマネージャ通報(TCP_IP In-Band)の宛先設定)を参照してください。
   TCP_IP Out-of-Band による通報をするときの宛先設定は、本書の 2 章(3.1.2. 通報手段がマネージャ通報(TCP_IP Out-of-Band)の宛先設定)を参照してください。

3. 監視イベントの設定、および、監視イベントへの通報先を結びつけます。
   エージェントイベントとは、ESMPRO/ServerAgent が検出した故障の監視イベントを指します。
   エージェントイベントの設定は、本書の 4 章(エージェントイベントの設定)を参照してください。
   Syslog イベントとは、Syslog 監視機能により検出した故障の監視イベントを指します。
   Syslog イベントの設定は、本書の 5 章(Syslog イベントの設定)を参照してください。

2. 基本設定

機　能

通報手段の有効/無効、マネージャ通報(SNMP)の Trap 送信先、エラー発生時のシャットダウン機能の有効/無効、シャットダウン開始までの時間を設定できます。通報手段を無効にすると、すべての監視イベントに設定されている当該通報手段による通報されなくなります。シャットダウンを無効にすると、ESMPRO/ServerManager からのリモートシャットダウン/リブートも無効となります。また、各監視イベントの通報後動作でシャットダウン/リブートが設定されているときも、通報発生後のシャットダウン/リブートが実行されなくなります。

設　定

コントロールパネル(ESMamsadm)の「通報基本設定」を選択して表示される[通報基本設定]画面にて、通報の基本設定ができます。



通報手段一覧

通報手段が表示されます。

その他の設定

設定項目が表示されます。

[クローズ]ボタン

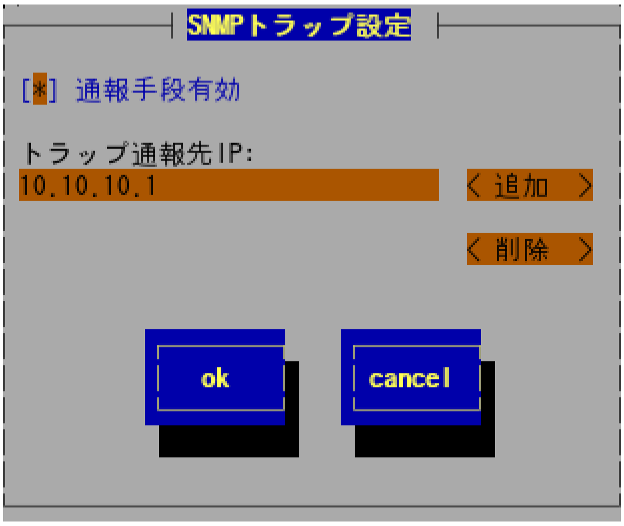
この画面を閉じます。

2.1 通報手段の設定

通報手段の有効/無効、マネージャ通報(SNMP)のトラップ通報先 IP が設定できます。

2.1.1 マネージャ通報(SNMP)の基本設定

[通報基本設定]画面の通報手段一覧から「マネージャ通報(SNMP)」を選択して表示される、[SNMP トラップ設定]画面にて、マネージャ通報(SNMP)の有効/無効、トラップ通報先 IP が設定できます。



通報手段有効

SNMP による通報手段の有効(チェックあり) と無効(チェックなし)が<スペース>キーで設定できます。既定値は"有効"です。

トラップ通報先 IP

通報先に設定している IP アドレスが一覧で表示されます。ESMPRO/ServerAgent から送信する Trap の宛先は、SNMP 設定ファイル(snmpd.conf)に設定される Trap Destination は使用しません。

[追加...]ボタン

トラップ通報先 IP に新しい通報先の IP アドレスを追加できます。

[削除...]ボタン

トラップ通報先 IP から削除したい通報先の IP アドレスを削除できます。

[ok]ボタン

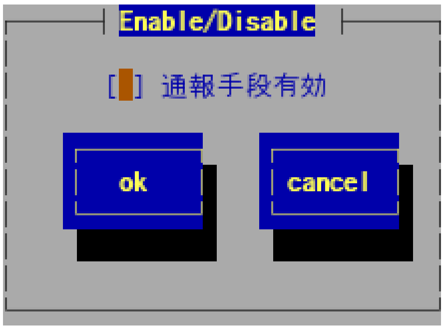
設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

2.1.2 マネージャ通報(TCP_IP In-Band)の基本設定

[通報基本設定]画面の通報手段一覧から「マネージャ通報(TCP_IP In-Band)」を選択して表示される、[Enable/Disable]画面にて、マネージャ通報(TCP_IP In-Band)の有効/無効が設定できます。



通報手段有効

TCP_IP In-Band による通報手段の有効(チェックあり)と無効(チェックなし)が<スペース>キーで設定できます。

[ok]ボタン

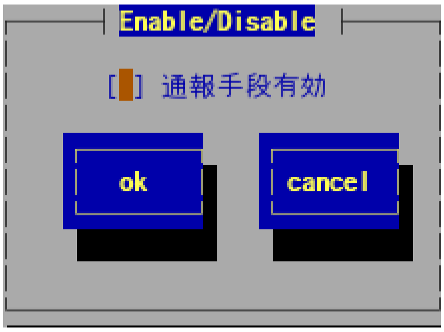
設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

2.1.3 マネージャ通報(TCP_IP Out-of-Band)の基本設定

[通報基本設定]画面の通報手段一覧から｢マネージャ通報(TCP_IP Out-of-Band)｣を選択して表示される、[Enable/Disable]画面にて、マネージャ通報(TCP_IP Out-of-Band)の有効/無効が設定できます。
TCP/IP Out-of-Band 通報を有効にするときは、ESMPRO/ServerManager 側の RAS(Remote Access Service)設定の暗号化の設定は、「クリアテキストを含む任意の認証を許可する」を必ず選択します。



通報手段有効

TCP_IP Out-of-Band による通報手段の有効(チェックあり)と無効(チェックなし)が<スペース>キーで設定できます。

[ok]ボタン

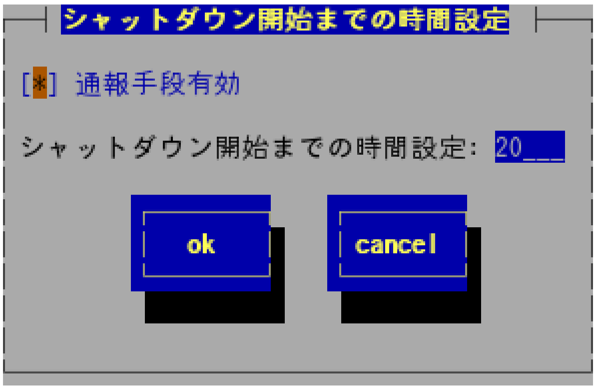
設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

2.1.4 その他の設定

[通報基本設定]画面のその他の設定から「シャットダウン開始までの時間設定」を選択して表示される、[シャットダウン開始までの時間設定]画面にて、シャットダウン開始までの時間が設定できます。



通報手段有効

通報によるシャットダウン機能の有効(チェックあり)と無効(チェックなし)が<スペース>キーで設定できます。
既定値は"有効"です。

シャットダウン開始までの時間設定

ESMPRO/ServerAgent が OS のシャットダウンを開始するまでの時間が設定できます。
既定値は 20 秒です。
設定可能範囲は 0～1800 秒です。
通報後のアクションにシャットダウンを指定しているとき、ESMPRO/ServerManager からシャットダウン指示があったとき、または、しきい値判定の結果シャットダウンするときは、ここで設定した時間が経過した後、OS のシャットダウンが開始します。

[ok]ボタン

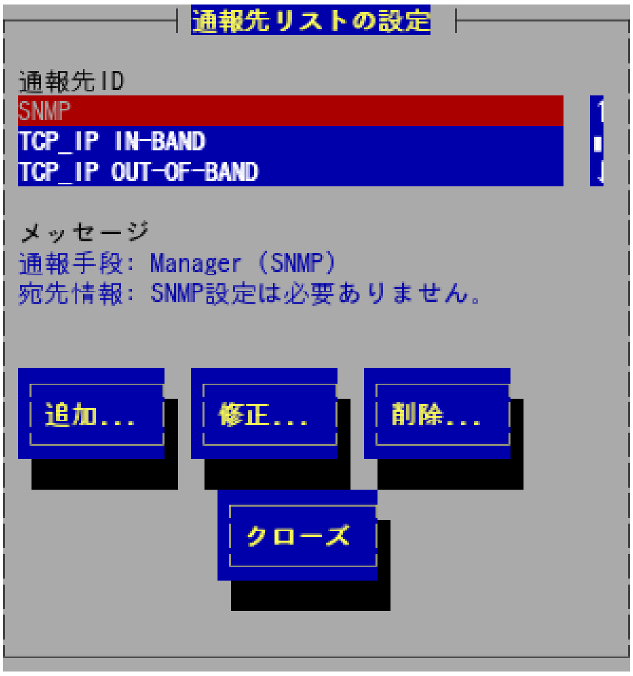
設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

3. 通報先リストの設定

コントロールパネル(ESMamsadm)の「通報先リストの設定」を選択して表示される[通報先リストの設定]画面にて、通報先 ID の設定変更、追加、削除および通報スケジュールが設定できます。



通報先 ID 一覧

通報先 ID のリストが表示されます。

メッセージ

通報手段：通報先 ID 一覧で選択された通報先 ID に設定されている通報手段が表示されます。
宛先情報：通報先 ID 一覧で選択された通報先 ID に設定されている宛先情報が表示されます。

[追加...]ボタン

通報先 ID を追加できます。[追加…]ボタンを押すと、[ID 設定] 画面が表示されます。
同一通報手段で異なる通報先を持つ通報先 ID を登録しておくと､同一手段で複数の宛先に通報できます。

[修正...]ボタン

通報先 ID 一覧で選択した通報先 ID に対して、通報先の設定が変更できます。
[修正…]ボタンを押すと、[ID 設定]画面が表示されます。

[削除...]ボタン

通報先 ID 一覧で選択した通報先 ID を削除できます。
通報先 ID を削除すると、各監視イベントに設定されている通報先 ID も削除されます。また、既定で設定している”SNMP”と”TCP_IP In-Band”、”TCP_IP Out-of-Band”の 3 つの通報先 ID は、削除できません。

[クローズ]ボタン

この画面を閉じます。

3.1 通報先IDの設定変更

通報先リストに登録されている通報先 ID の設定変更ができます。[通報先リストの設定]画面の通報先 ID 一覧で変更したい通報先 ID を選択し、[修正]ボタンを押すと[ID 設定]画面が開きます。設定内容は、通報手段によって異なります。



● **設定方法**

必要に応じて[宛先設定...]ボタンおよび[スケジュール...]ボタンを押して､宛先と通報スケジュールを設定します。

設定変更のとき、ID および通報手段の項目は、表示のみとなり、設定できません。

通報手段が「Manager(SNMP)」のときは、[宛先設定...]ボタンを押しても、ここでは設定する必要がないため、宛先設定画面は、表示されません。

3.1.1 通報手段がマネージャ通報(TCP_IP In-Band)の宛先設定

通報手段がマネージャ通報(TCP_IP In-Band)のとき、[ID 設定]画面で[宛先設定...]ボタンを押すと表示される[マネージャ(TCP_IP In-Band)設定]画面にて、宛先が設定できます。
/etc/hosts に自ホスト名が未設定のとき、ESMPRO/ServerAgent は UDP のソケット通信を利用して、TRAP 送信元の IP アドレスを取得します。
アラートビューアでホスト名が不明と表示されるときは、/etc/hosts ファイルに本機の IP アドレスと hostname を記載してください。

[記載例] 本機の IP アドレス：192.168.1.123, hostname：server1

192.168.1.123　　server1

/etc/hosts ファイルへの記載内容詳細は、6 章(よくある質問)の「ESMPRO/ServerManager のアラートビューアで受信した通報が「不明なサーバ」またはトラップの送信元と異なるサーバーが表示される。」項目を参照してください。



IP アドレス(またはホスト)

通報先の ESMPRO/ServerManager が導入されたマシンの IP アドレス(またはホスト名)を指定します。省略することはできません。

ポート番号

ソケット間通信で使用するポート番号を設定できます。
このポート番号は、ESMPRO/ServerAgent と通報先の ESMPRO/ServerManager で同じ値を設定してください。既定値は 31134 です。
既定値に問題がない限り、設定を変更しないでください。
既定値に問題があるとき、6001 から 65535 の範囲で番号を変更して、通報先の ESMPRO/ServerManager がインストールされているマシンで設定ツールを実行し、[通報基本設定]の[通報受信設定]-[エージェントからの受信(TCP/IP)]の設定を変更してください。

チェック
アクセス制御を設定している場合は、指定したポートのアクセスを許可してください。

[既定値]ボタン

ボタンを押すと、既定値が設定されます。

[ok]ボタン

設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

3.1.2 通報手段がマネージャ通報(TCP_IP Out-of-Band)の宛先設定

通報手段がマネージャ通報(TCP_IP Out-of-Band)のとき、[ID 設定]画面で[宛先設定...]ボタンを押すと表示される[マネージャ(TCP_IP Out-of-Band)設定]画面にて、宛先が設定できます。
/etc/hosts に自ホスト名が未設定のとき、ESMPRO/ServerAgent は UDP のソケット通信を利用して、TRAP 送信元の IP アドレスを取得します。
アラートビューアでホスト名が不明と表示されるときは、/etc/hosts ファイルに本機の IP アドレスと hostname を記載してください。
[記載例] 本機の IP アドレス：192.168.1.123, hostname：server1
192.168.1.123　　server1
/etc/hosts ファイルへの記載内容詳細は、6 章(よくある質問)の「ESMPRO/ServerManager のアラートビューアで受信した通報が「不明なサーバ」またはトラップの送信元と異なるサーバーが表示される。」項目を参照してください。



IP アドレス(またはホスト)
通報先の ESMPRO/ServerManager が導入されたマシンの IP アドレス(またはホスト名)を指定します。
省略することはできません。

リモートアクセスサービスのエントリ選択
接続先の電話番号と、接続時に必要なユーザー名、パスワードを設定できます。

ポート番号
ソケット間通信で使用するポート番号を設定できます。
このポート番号は、ESMPRO/ServerAgent と通報先の ESMPRO/ServerManager で同じ値を設定します。
既定値は 31134 です。
既定値に問題がない限り、設定を変更しないでください。
既定値に問題があるとき、6001 から 65535 の範囲で番号を変更して、通報先の ESMPRO/ServerManager がインストールされているマシンで設定ツールを実行し、[通報基本設定]の[通報受信設定]-[エージェントからの受信(TCP/IP)]の設定を変更してください。

チェック

アクセス制御を設定している場合は、指定したポートのアクセスを許可してください。

[既定値]ボタン

ボタンを押すと、既定値が設定されます。

[ok]ボタン

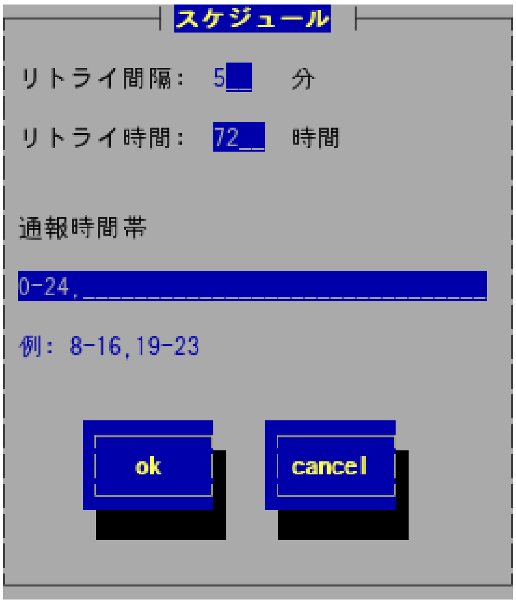
設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

3.1.3 スケジュール設定

通報先 ID ごとに、通報スケジュールが設定できます。



リトライ間隔

通報リトライをする間隔が設定できます。
既定値は 5 分です。
設定可能範囲は 1～30 分です。

リトライ時間

最大リトライ可能時間が設定できます。
0 を設定したときは、通報リトライしません。
既定値は 72 時間です。
設定可能範囲は 0～240 時間です。

通報時間帯

通報時間帯(24 時間表記の 1 時間単位)を指定してください。指定した時間帯に発生した故障のみを通報します。通報をしない時間帯に発生したイベントは通報されず、通報をする時間帯になると通報します。(それまでイベントの通報は保留されます。)
既定値は 0-24 で、24 時間通報可能となっています。

[ok]ボタン

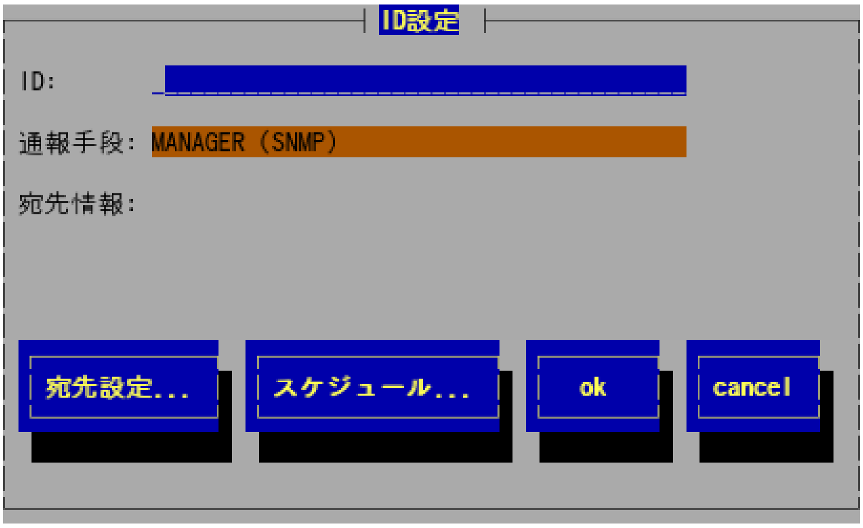
設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

3.1.4 通報先IDの追加

通報先 ID を追加します。設定内容は通報手段によって異なります。



< 設定手順 >

1) ID 名を入力します。
2) 通報手段を<↑>か<↓>キーで選択します。
3) [宛先設定...]ボタンを押し、表示される画面にて宛先を設定します。
4) [スケジュール...]ボタンを押し、表示される画面で通報スケジュールを設定します。
5) [ok]ボタンを押します。

通報手段で「Manager(SNMP)」を選択したときは、[宛先設定...]ボタンを押しても、ここでは設定する必要がないため、宛先設定画面は表示されません。

4. エージェントイベントの設定

機 能

エージェントイベントの設定および通報先を結びつけます。監視対象のイベントが発生したとき、ここで結びつけた通報先に通報されます。

設 定

コントロールパネル(ESMamsadm)の「エージェントイベントの設定」を選択して表示される[エージェントイベント設定]画面にて、エージェントイベントの設定ができます。



ソース名

ソース名を<↑>か<↓>キーで選択します。

ソースに対する処理

ソースに対する処理を<スペース>キーで選択できます。
本選択はエージェントイベント設定内容ではなく、処理方法の選択です。
そのため、コントロールパネルの起動毎に「OFF」が選択されます。

以下の設定をするとき「OFF」を選択します。
・選択した「ソース名」のイベント ID に対して、通報先や監視イベントを設定するとき。

以下の設定をするとき「ON」を選択します。
・選択した「ソース名」のイベント ID すべてに対して、一括で通報先を設定するとき。
　ただし、監視イベントの設定はできません。

イベント ID

「ソースに対する処理」で「OFF」を選択しているとき、「ソース名」で選択されたイベント ID を<↑>か<↓>キーで選択し表示します。
「ソースに対する処理」で「ON」を選択しているとき、「イベント ID」は「すべて」と表示されます。

Trap Name

選択された「イベント ID」のトラップ名を表示します。

[設定...]ボタン

[設定...]ボタンを押すと、[監視イベント設定]画面が表示されます。
「ソースに対する処理」で「OFF」を選択しているとき、選択したソースのイベント ID に対して、設定できます。
「ソースに対する処理」で「ON」を選択しているとき、選択したソースのイベント ID すべてに対して一括で通報先を設定できます。

[クローズ]ボタン

この画面を閉じます。

4.1 通報先の指定(エージェントイベント)

通報先の指定方法には、以下の方法があります。

1. 監視イベントごとに通報先を指定する方法（「ソースに対する処理」で「OFF」を選択しているとき)
2. ソースごとに通報先を一括指定する方法（「ソースに対する処理」で「ON」を選択しているとき)

4.1.1 監視イベントごとに通報先を指定する方法

通報先の設定と通報後の動作、対処法の設定ができます。

＜ 設定手順 ＞

1. コントロールパネル(ESMamsadm)を起動し、「エージェントイベントの設定」を選択します。
   [エージェントイベントの設定] 画面が表示されます。

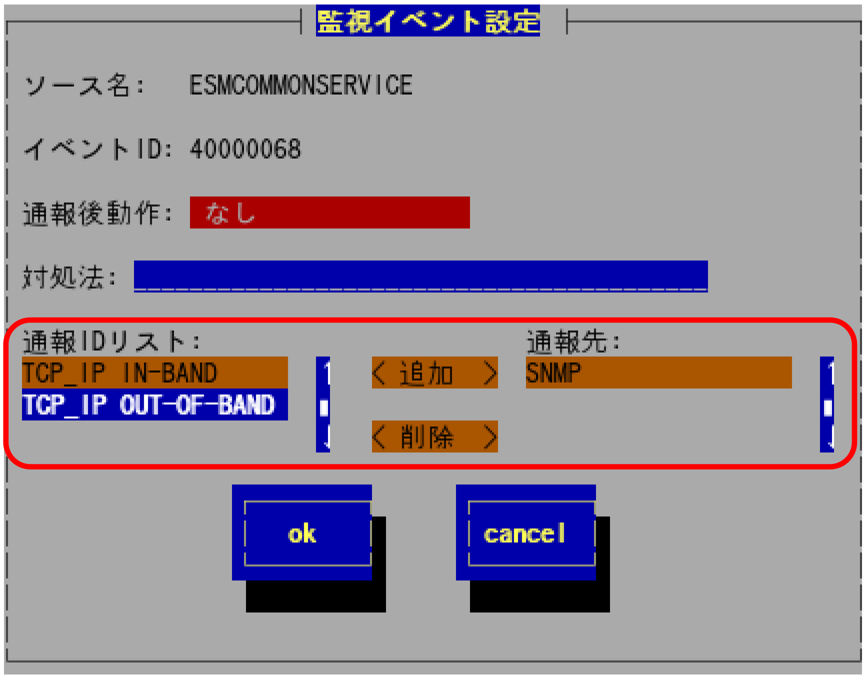


2. 「ソース名」でソースを<↑>か<↓>キーで選択します。

3. 「ソースに対する処理」で「OFF」に<スペース>キーでチェックします。

4. 「イベント ID」で設定したいイベント ID を<↑>か<↓>キーで選択します。

5. [設定...]ボタンを押します。
   [監視イベント設定] 画面が表示されます。



6. 「通報 ID リスト」から通報したい通報 ID を選択します。
   通報先の設定として、通報先に EXPRESSREPORT を追加できますが、Alive レベルが対象外のため、実際にエクスプレス通報されません。

7. [追加]ボタンを押します。
   通報 ID が「通報先」から「通報 ID リスト」に移動します。

8. 通報 ID を通報対象から削除するには「通報先」から通報 ID を選択して、[削除]ボタンを押します。
   通報 ID が「通報先」から「通報 ID リスト」に移動します。

9. [ok]ボタンを押します。

通報後動作

通報後の動作を設定できます。通報後の動作とは、このイベントが発生した後の動作を指し、「シャットダウン」「リブート」「何もしない」の 3 つから<↑>か<↓>キーで選択します。

対処法

通報する項目に対する対処方法を設定できます。507 バイト(半角文字で 507 文字、全角文字で 253 文字)以下で指定します。日本語は使用できます。

4.1.2 ソースごとに通報先を一括指定する方法

ソースごとに通報先を一括で設定した後、再度、[監視イベント設定]画面を開いても、通報先一覧には何も表示されません。通報先の確認は「監視イベントごとに通報先を指定する方法」にて、個々のイベントを確認してください。

< 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「エージェントイベントの設定」を選択します。
   [エージェントイベントの設定] 画面が表示されます。



2. 「ソース名」でソースを<↑>か<↓>キーで選択します。

3. 「ソースに対する処理」で「ON」に<スペース>キーでチェックします。

4. [設定...]ボタンを押します。
   [監視イベント設定]画面が表示されます。



5. 「通報 ID リスト」から通報したい通報 ID を選択します。

6. [追加]ボタンを押します。
   通報 ID が「通報 ID リスト」から「通報先」に移動します。

7. 通報 ID を通報対象から削除するには「通報先」から通報 ID を選択して、[削除]ボタンを押します。
   通報 ID が「通報先」から「通報 ID リスト」に移動します。

8. [ok]ボタンを押します。

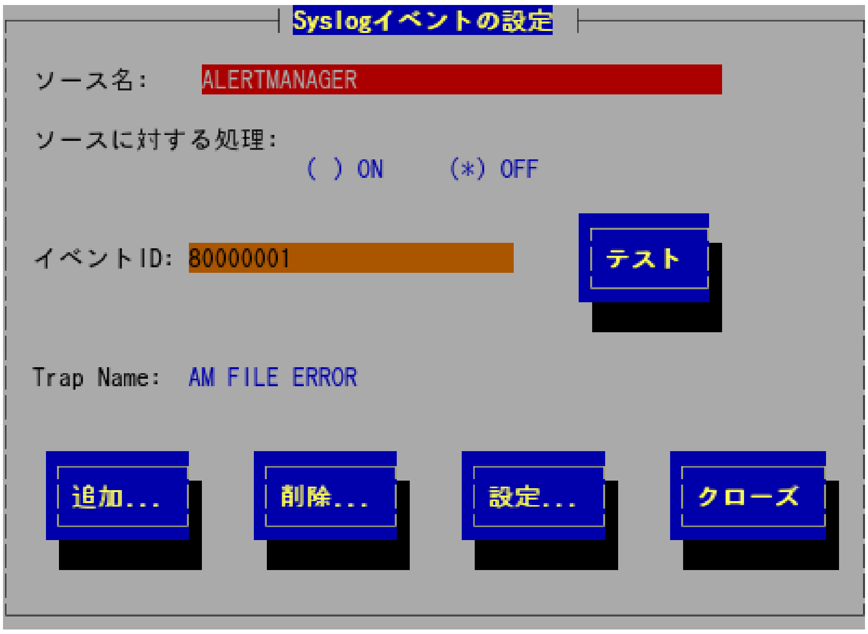
5. Syslogイベントの設定

機 能

Syslog イベントの設定および通報先を結びつけます。監視対象のイベントが発生したとき、ここで結びつけた通報先に通報されます。Syslog イベントは、あらかじめ登録されているイベント以外に、システム環境に応じて新たなソース、監視イベントを任意に追加や削除できます。Syslog 監視は既定値では 300 秒間隔で監視しています。Syslog 監視の監視間隔は変更できます。Syslog 監視の監視間隔の設定方法につきましては本書の 2 章(3. Syslog 監視)を参照してください。

設 定

コントロールパネル(ESMamsadm)の「Syslog イベントの設定」を選択して表示される[Syslog イベントの設定]画面にて、Syslog イベントの設定ができます。



ソース名

ソースを<↑>か<↓>キーで選択し表示します。

ソースに対する処理

ソースに対する処理を<スペース>キーで選択できます。
本選択は Syslog イベントの設定内容ではなく、処理方法の選択です。
そのため、コントロールパネルの起動毎に「OFF」が選択されます。

以下の設定をするとき「OFF」を選択します。
・選択した「ソース名」のイベント ID に対して、通報先や監視イベントを設定するとき。
・監視イベントの追加や削除をするとき。

以下の設定をするとき「ON」を選択します。
・選択した「ソース名」のイベント ID すべてに対して、一括で通報先を設定するとき。
　ただし、監視イベントの設定はできません。

・ソースの追加や削除(すべての監視イベントを削除)をするとき。

イベント ID

「ソースに対する処理」で「OFF」を選択しているときは、「ソース名」で選択されたイベント ID を<↑>か<↓>キーで選択し表示します。
「ソースに対する処理」で「ON」を選択しているときは、「イベント ID」に「すべて」と表示します。

Trap Name

選択されたイベント ID のトラップ名を表示します。

[クローズ]ボタン

[Syslog イベントの設定]画面を閉じます。
[クローズ]ボタンを押すと、Syslog 監視の間隔はリセットされ、[クローズ]ボタンを押した時間から Syslog 監視間隔(既定値は 300 秒)までは、Syslog イベントを検知しません。

[追加...]ボタン

[追加...]ボタンを押すと、[Syslog イベントの追加]画面が表示されます。
「ソースに対する処理」で「OFF」を選択しているときは、選択したソースの監視イベントを追加します。
「ソースに対する処理」で「ON」を選択しているときは、ソースを含め監視イベントを追加します。

[削除...]ボタン

[削除...]ボタンを押すと、
「ソースに対する処理」で「OFF」を選択しているときは、選択したソースの監視イベントを削除します。
「ソースに対する処理」で「ON」を選択しているときは、ソースを含め監視イベントすべてを削除します。

[設定...]ボタン

[設定...]ボタンを押すと、[Syslog アプリケーション設定]画面が表示されます。
「ソースに対する処理」で「OFF」を選択しているときは、選択したソースのイベント ID に対して、設定変更および通報先を設定できます。
「ソースに対する処理」で「ON」を選択しているときは、選択したソースのイベント ID すべてに対して、一括で通報先を設定できます。

[テスト]ボタン

「ソースに対する処理」で「OFF」を選択しているときは、選択した Syslog イベントのキーワードを含む"ESMamsadm: [TEST - AlertManager] (キーワード)"文字列を syslog に記録することにより、テストイベントを発生させて、監視対象イベントに結び付けた宛先への通報を実際にシミュレートできます。通報のみならず「通報後動作」も動作します。そのため、設定によってはシャットダウンされることもありますので、テストする通報の選択にはご注意ください。
「ソースに対する処理」で「ON」を選択しているとき、または特定のソース名(FTREPORT)のイベントは、テストできません。

Syslog イベントの追加や削除、設定を変更したときは、Syslog イベントの情報を再読み込みさせる必要があります。[クローズ]ボタンを押して、[Syslog イベントの設定]画面を閉じ、[通報設定]画面から、再度「Syslog イベントの設定」を選択します。その後、[テスト]ボタンを押します。

5.1 通報先の指定(Syslogイベント)

通報先の指定方法には、以下のふたとおりの方法があります。

1. 監視イベントごとに通報先を指定する方法(「ソースに対する処理」で「OFF」を選択しているとき)
2. ソースごとに通報先を一括指定する方法(「ソースに対する処理」で「ON」を選択しているとき)

5.1.1 監視イベントごとに通報先を指定する方法

監視イベントごとに個別に通報先を指定するときの方法を説明します。
通報先の設定と同時に、通報後の動作、対処法等の設定もできます。

< 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し､｢Syslog イベントの設定｣を選択します。

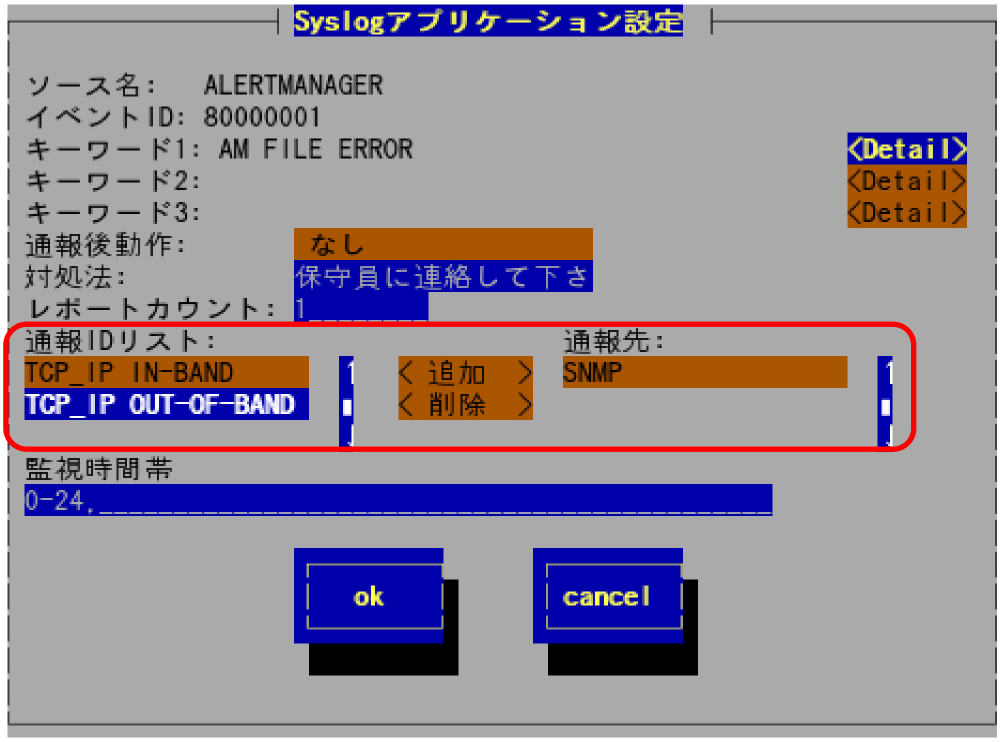


2. 「ソース名」でソースを<↑>か<↓>キーで選択します。

3. 「ソースに対する処理」で「OFF」に<スペース>キーでチェックします。

4. 「イベント ID」で設定したいイベント ID を<↑>か<↓>キーで選択します。

5. [設定...]ボタンを押します。
   [Syslog アプリケーション設定] 画面が表示されます。



6. 「通報 ID リスト」から通報したい通報 ID を選択します。
   通報先の設定として、通報先に EXPRESSREPORT を追加できますが、Alive レベルが対象外のため、実際にエクスプレス通報されません。

7. [追加]ボタンを押します。
   通報 ID が「通報 ID リスト」から「通報先」に移動します。

8. 通報 ID を通報対象から削除するには「通報先」から通報 ID を選択して、[削除]ボタンを押します。
   通報 ID が「通報先」から「通報 ID リスト」に移動します。

9. [ok]ボタンを押します。

通報後動作

通報後のアクションを設定できます。[通報後のアクション]とは、このイベントが発生した後の動作を指し、「シャットダウン」「リブート」「何もしない」の 3 つから<↑>か<↓>キーで選択します。

対処法

通報する項目に対する対処方法を設定します。507 バイト(半角文字で 507 文字、全角文字で 253 文字)以下で指定します。日本語は使用できます。

レポートカウント

同一イベントを指定回数検出したときに通報をします。

監視時間帯

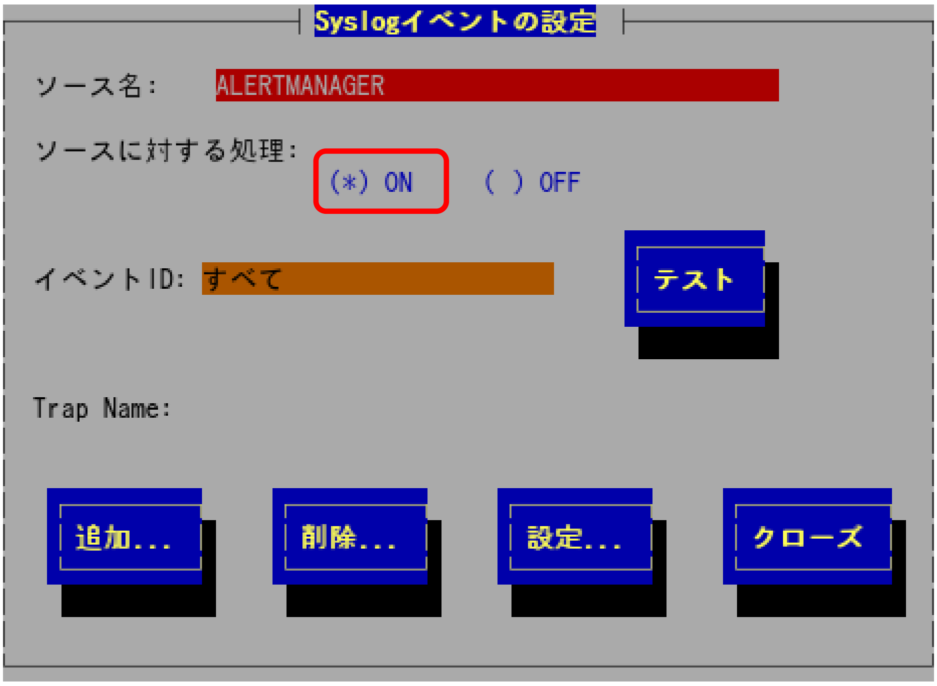
監視時間帯を指定できます。指定した時間帯に発生したイベントのみを通報します。
時間設定は 1 時間単位で指定できます。既定値では 24 時間通報可能となっています。

5.1.2 ソースごとに通報先を一括指定する方法

ソースごとに、ソース配下のすべての監視イベントに同じ通報先を一括して指定する方法を説明します。通報先を一括で設定した後、再度、[Syslog アプリケーション設定]画面を開いても、通報先一覧には何も表示されません。通報先の確認は「監視イベントごとに個別に通報先を指定する方法」にて、個々のイベントで確認します。

＜ 設定手順 ＞

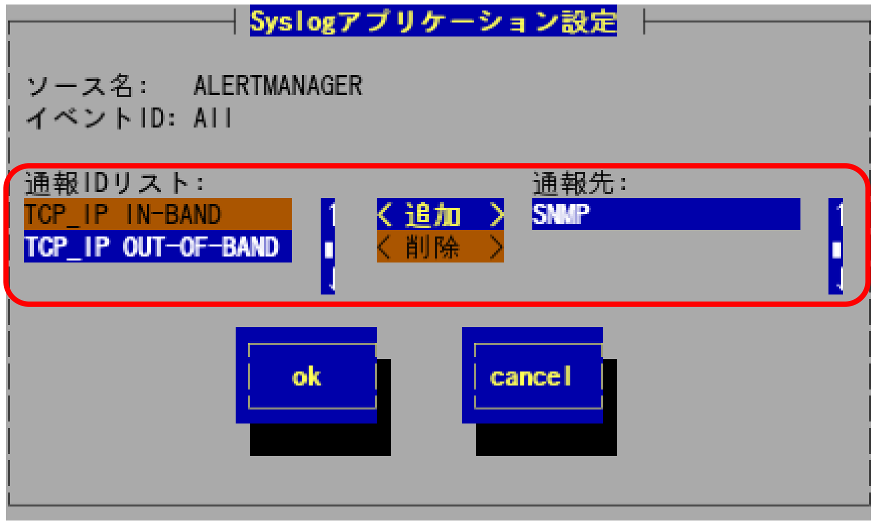
1. コントロールパネル(ESMamsadm)を起動し､｢Syslog イベントの設定｣を選択します。



2. 「ソース名」でソースを<↑>か<↓>キーで選択します。

3. 「ソースに対する処理」で「ON」に<スペース>キーでチェックします。

4. [設定...]ボタンを押します。
   [Syslog アプリケーション設定] 画面が表示されます。



5. 「通報 ID リスト」から通報したい通報 ID を選択します。

6. [追加]ボタンを押します。
   通報 ID が「通報 ID リスト」から「通報先」に移動します。

7. 通報 ID を通報対象から削除するには「通報先」から通報 ID を選択して、[削除]ボタンを押します。
   通報 ID が「通報先」から「通報 ID リスト」に移動します。

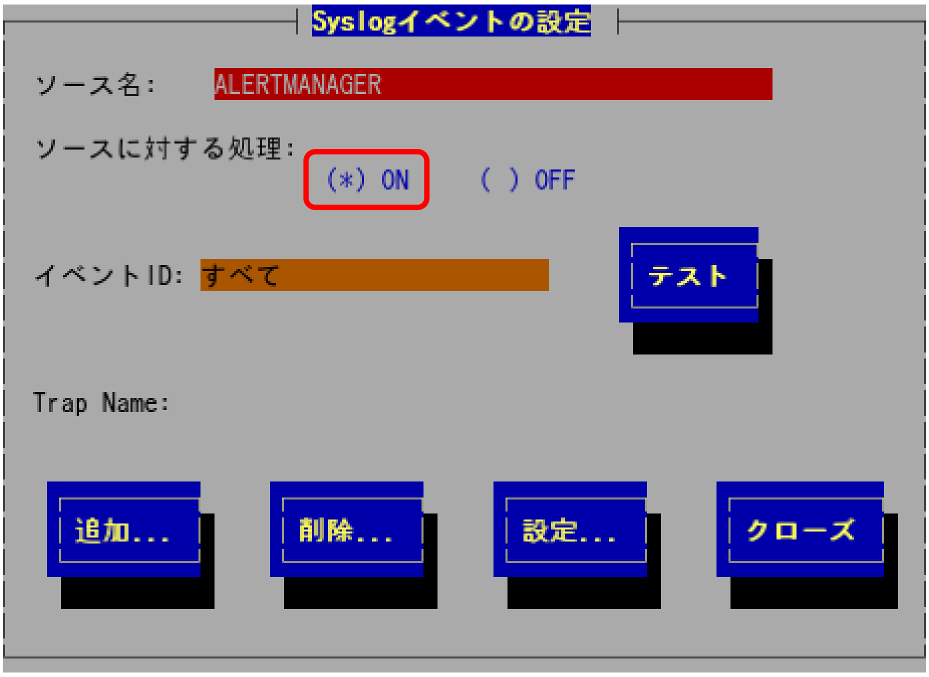
8. [ok]ボタンを押します。

5.2 Syslogイベントのソースの追加

システム環境に応じて、新たな Syslog イベントのソースを任意に追加できます。ESMPRO/ServerAgent 以外のアプリケーションが登録するイベントを監視したいときに設定します。ソース登録と同時に、1 件目の監視イベントをあわせて登録します。1 サーバーに登録できるソース名の個数は他の製品が登録するソース名の個数も含めて、最大で 1024 個ですが、登録件数によりディスク使用量・メモリ使用量が増加しますので、設定には注意してください。

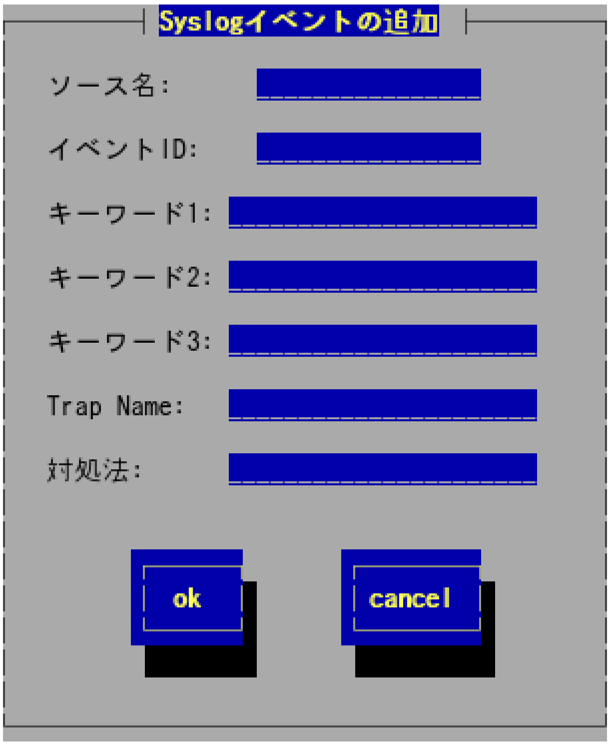
< 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「Syslog イベントの設定」を選択します。
   [Syslog イベントの設定] 画面が表示されます。



2. 「ソースに対する処理」で「ON」に<スペース>キーでチェックします。

3. [追加...]ボタンを押します。
   [Syslog イベントの追加] 画面が表示されます。



4. 「ソース名」「イベント ID」「キーワード」「Trap Name」「対処法」を設定します。

5. [ok]ボタンを押します。
   このとき、「通報後動作：なし」「レポートカウント：1」e が設定されます。

ソース名 (必須項目)

ソース名を 40 文字以下の半角英字で始まる半角英数字(大文字)で指定します。ソース名は大文字使用しますので、小文字を設定しても大文字に変換しますが、アラートビューアで表示する「タイプ」と「製品名」は設定した半角英数字のままとなります。小文字で設定したとき、「ソース」は大文字、「タイプ」と「製品名」は小文字となります。
ESMPRO/ServerManager のアラートビューアの「ソース」と「タイプ」、「製品名」欄に表示されます。

イベント ID (必須項目)

以下の命名規則に従って、半角英数字 8 文字(16 進数表記[0-9,A-F])で指定します。
＜監視イベント ID 命名規則＞
“x0000yyy”形式で指定します。(例：40000101、800002AB、C0000101)
“x”には、4,8,C の中から設定します。それぞれの意味は以下のとおりです。
4 ：情報系イベントを意味します。
ESMPRO/ServerManager のアラートビューアのアイコンが「緑色」で表示されます。
8 ：警告系イベントを意味します。
ESMPRO/ServerManager のアラートビューアのアイコンが「黄色」で表示されます。
C ：異常系イベントを意味します。
ESMPRO/ServerManager のアラートビューアのアイコンが「赤色」で表示されます。
“yyy”には、0x001(1)～0xFFF(4095)の範囲内で任意の 16 進数値を設定します。

キーワード 1 (必須項目)、キーワード 2、キーワード 3

syslog に記録されるメッセージを一意に特定できる文字列を、それぞれ 256 文字以下の半角英数字で指定します。すべてのキーワードを含むメッセージを syslog から検出したときに、そのメッセージの全文を ESMPRO/ServerManager に通報します。
ESMPRO/ServerManager のアラートビューアの「詳細」欄に表示されます。

Trap Name (必須項目)

通報メッセージの概要を 79 バイト(半角文字で 79 文字、全角文字で 39 文字)以下で指定します。日本語は使用できます。
ESMPRO/ServerManager のアラートビューアの「概要」欄に表示されます。

対処法

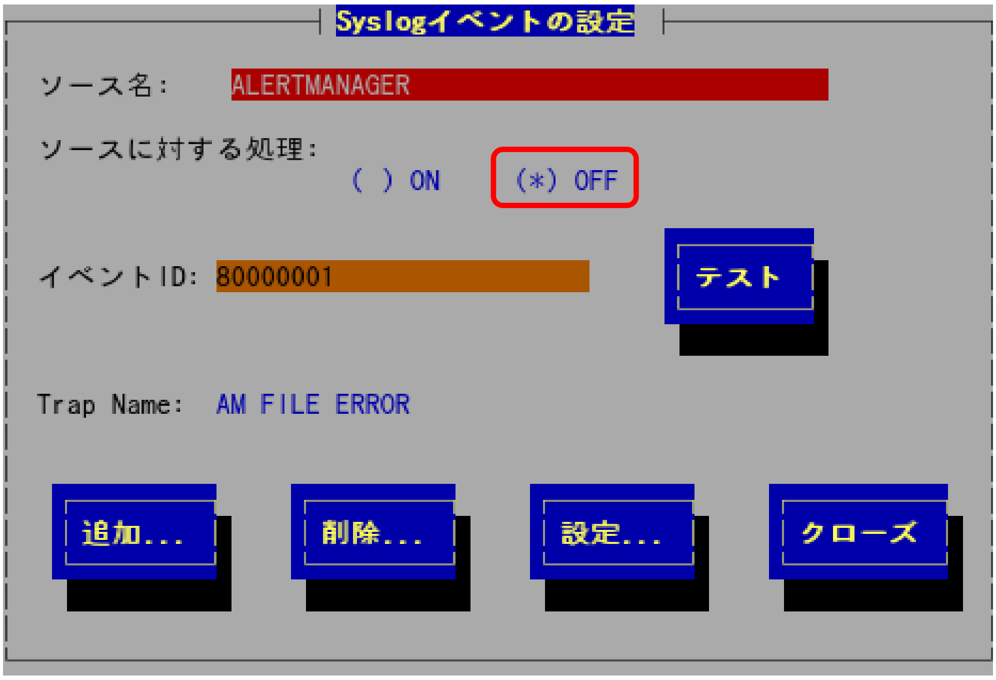
通報メッセージを受けたときの対処方法を 507 バイト(半角文字で 507 文字、全角文字で 253 文字)以下で指定します。日本語は使用できます。
ESMPRO/ServerManager のアラートビューアの「対処」欄に表示されます。

5.3 Syslogイベントの追加

すでに登録済みの Syslog イベントのソース配下に、システム環境に応じて新たな Syslog イベントを追加できます。

< 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し､｢Syslog イベントの設定｣を選択します。
   [Syslog イベントの設定] 画面が表示されます。



2. 「ソース名」でソース名を<↑>か<↓>キーで選択します。

3. 「ソースに対する処理」で「OFF」に<スペース>キーでチェックします。

4. [追加...]ボタンを押します。
   [Syslog イベントの追加] 画面が表示されます。

5. 「イベント ID」「キーワード」「Trap Name」「対処法」を設定します。
   各項目の設定内容は「5.2. Syslog イベントのソースの追加」に記載してある内容と同じです。

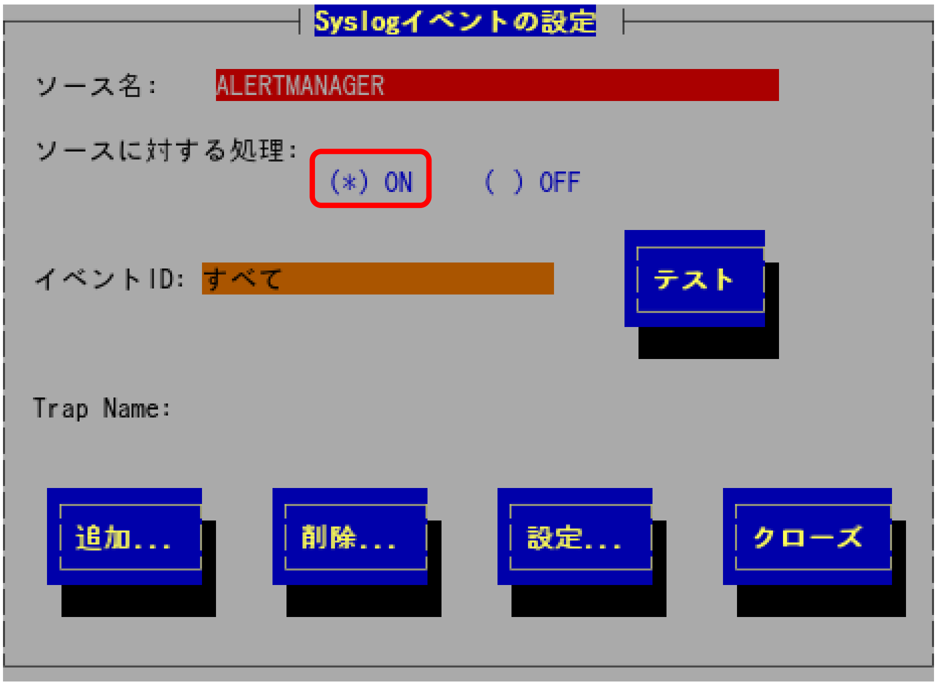
6. [ok]ボタンを押します。

5.4 Syslogイベントのソースの削除

Syslog イベント監視から、Syslog イベントのソースを削除できます。ソースを削除すると、その配下に登録されているすべての監視イベントも削除されます。また、ESMPRO/ServerAgent が登録している既定のソースを削除することはできません。

< 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し､｢Syslog イベントの設定｣を選択します。[Syslog イベントの設定] 画面が表示されます。



2. 「ソース名」で削除したいソース名を<↑>か<↓>キーで選択します。

3. 「ソースに対する処理」で「ON」に<スペース>キーでチェックします。

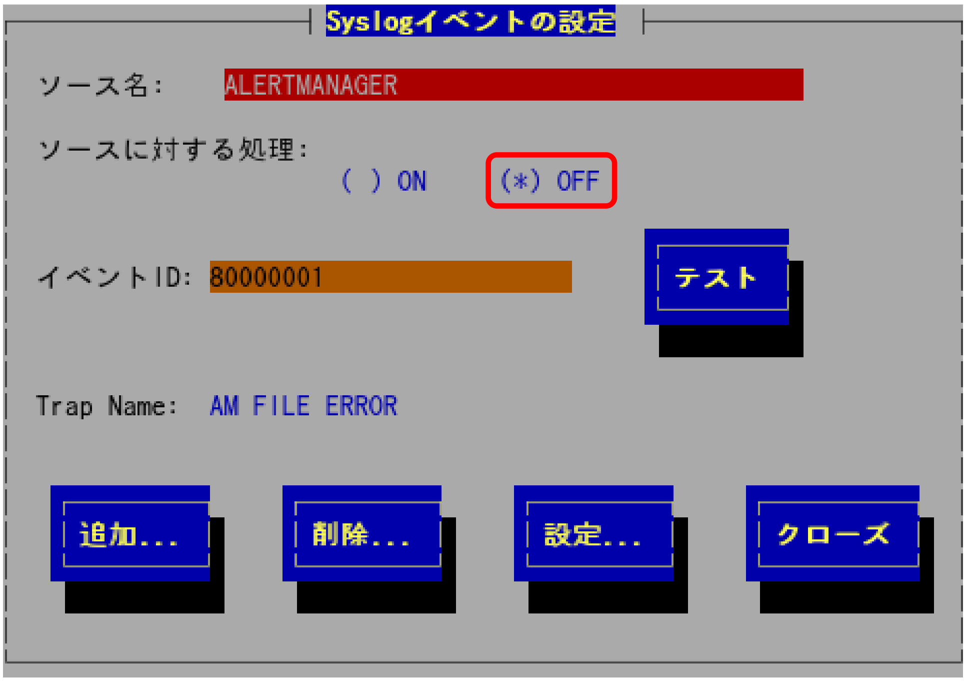
4. [削除...]ボタンを押します。

5.5 Syslogイベントの削除

Syslog イベント監視から、Syslog イベントを削除できます。ESMPRO/ServerAgent が登録している既定の監視イベントを削除することはできません。

< 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し､｢Syslog イベントの設定｣を選択します。
   [Syslog イベントの設定] 画面が表示されます。



2. 「ソース名」でソース名を<↑>か<↓>キーで選択します。

3. 「ソースに対する処理」で「OFF」に<スペース>キーでチェックします。

4. ｢イベント ID｣で削除したいイベント ID を<↑>か<↓>キーで選択します。

5. [削除...]ボタンを押します。

ESMPRO/ServerAgent Ver. 4.5

4 追加機能

ESMPRO/ServerAgent の追加機能について説明します。

1. OpenIPMI を利用した OS ストール監視

2. コンフィグレーションツール

1. OpenIPMIを利用したOSストール監視

本章では、OpenIPMI を利用した OS ストール監視を説明しています。

機　能

装置に搭載されているウォッチドックタイマー(ソフトウェアストール監視用タイマー)を定期的に更新することにより、OS の動作状況を監視します。OS のストールなどにより応答がなくなり、タイマーの更新がされなくなると、タイマーがタイムアウトして自動的にタイムアウト後の動作に設定された復旧方法を実行します。

チェック

本章の設定をする前に、必ず OpenIPMI の動作状況を確認してください。
lsmod コマンドで”mainte”が表示されているときは、サーバーマネージメントドライバーを利用して OS ストール監視をしているため、本章の設定をする必要はありません。

対　象　O S

Red Hat Enterprise Linux 4 (以降、RHEL4 と表記します)
Red Hat Enterprise Linux 5 (以降、RHEL5 と表記します)
SUSE Linux Enterprise Server 10 SP2 (以降、SLES10SP2 と表記します)
SUSE Linux Enterprise Server 10 SP3 (以降、SLES10SP3 と表記します)

設　定

ストール監視のタイムアウト、更新時間およびストール発生時の動作が設定できます。これによって OS 稼働中にストールが発生したときの復旧方法を設定できます。設定パラメーターは以下のとおりです。

タイムアウト時間：timeout

OS がストールしたと判定する時間を秒数で設定してください。
既定値は 60 秒です。10 秒より設定可能です。
/etc/sysconfig/ipmi ファイルにて設定できます。

タイムアウト後の動作：action

タイムアウト後の復旧方法を選択してください。既定値は「reset」です。
/etc/sysconfig/ipmi ファイルにて設定できます。

none	何もしません。
reset	システムをリセットし再起動を試みます。
power_off	システムの電源を切断します。
power_cycle	いったん電源 OFF し、直後に再度電源 ON します。

更新間隔：interval

タイムアウト時間のタイマーを更新する間隔を秒数で設定してください。
既定値は 10 秒です。設定可能範囲は 1～59 秒です。
/etc/watchdog.conf ファイルにて設定できます。

重要 **使用するマシンの負荷状況によっては、OS がストール状態でなくても、ウォッチドッグタイマの更新ができずにタイムアウトが発生する可能性があります。ご使用環境にて高負荷状態での評価した上でストール監視を設定してください。**

■ストール監視機能の設定手順

root 権限のあるユーザーでログインして、設定をしてください。

1.　必要なパッケージを事前にインストールしてください。

1.1　下記の OpenIPMI パッケージをインストールしてください。

RHEL4, RHEL5	SLES10SP2, SLES10SP3
- OpenIPMI-*.rpm	- OpenIPMI-*.rpm
- OpenIPMI-tools-*.rpm	- ipmitool-*.rpm

1.2　watchdog パッケージ(watchdog-*.rpm)をインストールしてください。
ご使用中の Linux によっては提供されていないときがあります。
watchdog パッケージがないときには、(3)の設定方法が異なります。

2.　OpenIPMI を設定してください。

2.1　以下を参考にして OpenIPMI の環境設定ファイル(/etc/sysconfig/ipmi)を vi コマンド等で修正してください。

```
----------------------------------------
IPMI_WATCHDOG=yes
IPMI_WATCHDOG_OPTIONS="timeout=180 action=reset start_now=1"
----------------------------------------
```

※この例では設定パラメーターは以下となっています。
　タイムアウト時間　　　：180 秒
　タイムアウト後の動作　：reset
　start_now が 1 にセットされたとき、ウォッチドッグタイマーは OpenIPMI ドライバーがロードされると同時に実行されます。

2.2　OpenIPMI を自動起動できるように設定してください。

```
# chkconfig ipmi on
```

3.　WDT(Watchdog Timer)更新プログラムを設定してください。
watchdog パッケージのインストールの有無によって、設定方法が異なりますので、それぞれのときについて述べます。

●watchdog パッケージがインストールされているとき

3.1　以下を参考にして watchdog の環境設定ファイル(/etc/watchdog.conf) を vi コマンド等で修正してください。

重要 **タイムアウト時間を指定できる watchdog パッケージを使用する場合は、IPMI の設定にかかわらず、タイムアウト時間は 60 秒(default)に再設定されます。このタイムアウト時間を変更する場合は、watchdog.conf に、下記の指定が必要です。**
**　watchdog-timeout =180→タイムアウト時間を秒数で指定(この場合は 180 秒を指定)**
タイムアウト時間指定の有無は、man watchdog.conf で watchdog-timeout の説明の有無で確認できます。

[タイムアウト時間を指定できない watchdog パッケージの場合]

----

watchdog-device = /dev/watchdog
interval = 30

[タイムアウト時間を指定できる watchdog パッケージの場合]
----
watchdog-device = /dev/watchdog
interval = 30
watchdog-timeout =180→タイムアウト時間を秒数で指定(この場合は 180 秒を指定)

※interval に更新間隔を秒数で設定してください。
この例では更新間隔は 30 秒となります。
尚、実測ではこの指定の半分の時間で更新されることが確認されています。

3.2 WDT 更新プログラムを自動起動できるように設定してください。

```
# chkconfig watchdog on
```

●watchdog パッケージがインストールされていないとき

3.1 下記の例を参考に、WDT 更新プログラムを作成してください。
この例ではファイル名を「ResetWDT」とします。

```
----------------------------------------
#!/bin/sh
while true
do
/usr/bin/ipmitool raw 0x6 0x22 > /dev/null 2>&1
sleep 30
done
----------------------------------------
```

※sleep の時間が更新間隔に相当し秒数で設定してください。
この例では更新間隔は 30 秒となります。

3.2 WDT 更新プログラムを/usr/sbin ディレクトリー配下にコピーしてください。

```
# install -p -m 755 ResetWDT /usr/sbin
```

3.3 下記の例を参考に、WDT 更新プログラムの起動スクリプトファイル(以降「WDT 起動スクリプト」という)を作成してください。
この例ではファイル名を「watchdog」とします。

```
----------------------------------------
#! /bin/sh
#
# chkconfig: - 27 46
# description: software watchdog
#
# Source function library.
. /etc/rc.d/init.d/functions                → SLES10SP2,SLES10SP3 では、本行は不要です。
prog=/usr/sbin/ResetWDT

case "$1" in
    start)
        echo -n "Starting watchdog daemon: "
        ${prog} &
        success "Starting watchdog daemon"  → SLES10SP2,SLES10SP3 では、本行は不要です。
```

```
            echo
            ;;
        *)
            echo "Usage: watchdog {start}"
            exit 1
            ;;
esac
----------------------------------------
```

「prog=」に WDT 更新プログラム(この例では ResetWDT)の格納パスを指定してください。

3.4 上記の WDT 起動スクリプトを install コマンドでコピーしてください。
RHEL4, RHEL5 では、以下のコマンドで/etc/rc.d/init.d ディレクトリディレクトリー配下にコピーしてください。

```
# install -p -m 755 watchdog /etc/rc.d/init.d
```

SLES10SP2, SLES10SP3 では、以下のコマンドで/etc/init.d ディレクトリディレクトリー配下にコピーしてください。

```
# install -p -m 755 watchdog /etc/init.d
```

3.5 WDT 更新プログラムを自動起動できるように設定してください。

```
# chkconfig –-add watchdog
# chkconfig watchdog on
```

チェック

Windows OS 上で、上記のプログラムおよびスクリプトファイルを作成するときには、ご使用中の Linux に対応したコードに変換してください。

4. OS を再起動してください。再起動にてストール監視機能が有効となります。

```
# reboot
```

■ストール監視機能を無効にする手順
root 権限のあるユーザーでログインして、設定をしてください。

1. 以下を参考にして OpenIPMI の環境設定ファイル(/etc/sysconfig/ipmi)を vi コマンド等で修正してください。

```
----------------------------------------
IPMI_WATCHDOG=no
----------------------------------------
```

2. WDT 更新プログラムを自動起動しないように設定してください。

3. OS を再起動してください。再起動にてストール監視機能が無効となります。

■ストール監視機能の関連モジュールを削除する手順
root 権限のあるユーザーでログインして、設定をしてください。

1. ストール監視機能を無効にしてください。

2. watchdog パッケージがインストールされているときは、削除してください。
インストールされていないときは、以下をしてください。

3. WDT 更新プログラムおよび WDT 起動スクリプトを削除してください。

対 象 OS

SUSE Linux Enterprise Server 11 SP1 (以降、SLES11SP1 と表記します)
Red Hat Enterprise Linux 6 (以降、RHEL6 と表記します)

設 定

■ストール監視機能の設定手順

root 権限のあるユーザーでログインして、設定をしてください。

1. 必要なパッケージを事前にインストールしてください。

1.1 下記の OpenIPMI パッケージをインストールしてください。

SLES11SP1, RHEL6
- OpenIPMI-*.rpm
- ipmitool-*.rpm

2. OpenIPMI を設定してください。

2.1 以下を参考にして OpenIPMI の環境設定ファイル(/etc/sysconfig/ipmi)を vi コマンド等で修正してください。

SLES11SP1, RHEL6.0 では下記を yes に設定しても起動時にエラーとなることが確認されています。

```
----------------------------------------
IPMI_WATCHDOG=no
----------------------------------------
```

2.2 OpenIPMI を自動起動できるように設定してください。

```
# chkconfig ipmi on
```

3. WDT (Watchdog Timer)更新プログラムを設定してください。

3.1 下記の例を参考に、WDT 更新プログラムを作成してください。

この例ではファイル名を「ResetWDT」とします。

```
----------------------------------------
#!/bin/sh
sleep 60      ← ご使用中の環境に合わせて WDT 開始の待ち時間を設定してください。
/usr/bin/ipmitool raw 0x6 0x24 0x4 0x01 0xa 0x3e 0x08 0x07 > /dev/null 2>&1   ※1
while true
do
/usr/bin/ipmitool raw 0x6 0x22 > /dev/null 2>&1
sleep 30      ← 更新間隔に相当。秒数で指定してください。この例では 30 秒です。
done
----------------------------------------
```

※1 Set Watchdog Timer コマンド実行時の ipmitool の引数は以下のとおりです。

raw ... IPMI コマンドを指定して実行する際の引数(固定)
0x6 ... NetFunction (固定)
0x24 ... Command (固定)

NetFunction(0x6) と Command(0x24) の組合せで、
Set Watchdog Timer コマンドを表します。

0x4 ... Timer Use

OS 動作中のストール監視のとき 0x4 から変更の必要はありません。
下位 3 ビットで、ストール監視のフェーズを表しています。

[2:0]

000b = reserved
001b = BIOS FRB2
010b = BIOS/POST
011b = OS Load
100b = SMS/OS
101b = OEM
上記以外 = reserved (使用しません)

0x01 ... Timer Actions

上位 4 ビットでタイムアウト発生時の動作設定をします。

[7] reserved

[6:4] pre-timeout interrupt

000b = none(何もしません)
001b = SMI (使用しません)
010b = NMI/Diagnostic Interrupt (NMI を発生します)
011b = Messaging Interrupt (使用しません)
上記以外 = reserved(使用しません)

下位 4 ビットでタイムアウト発生後の動作設定をします。

[3] reserved

[2:0] timeout action

000b = no action (何もしません)
001b = Hard Reset (リセットします)
010b = Power Down (DC OFF します)
011b = Power Cycle (DC OFF 後、DC ON します)
上記以外 = reserved(使用しません)

0xa ... Pre-timeout interval

タイムアウト検出からタイムアウト後の動作に移行するまでの
時間を 1 秒単位で指定します。0xa のときは 10 秒となります。

0x3e ... Timer Use Expiration flags clear

通常は 0x3e のまま、変更の必要はありません。

0x08 ... Initial countdown value, lsbyte(100ms/count)

0x07 ... Initial countdown value, msbyte

Initial countdown value で、カウントダウン時間を設定します。
BMC のウォッチドッグタイマタイマー機能は、1 count は 100 ミリ秒単位と
なっているため、カウントダウン時間を 180 秒に設定するとき、
180 x 10 = 1800(10 進数) = 0x0708(16 進数)
lsbyte, msbyte の順に引数に指定するので 0x08 0x07 の順となる。

重要

使用するマシンの負荷状況によっては、OS がストール状態でなくても、ウォッチドッグタイマの更新ができずにタイムアウトが発生する可能性があります。ご使用環境にて高負荷状態での評価した上でストール監視を設定してください。

ヒント

コマンドの詳細は IPMI 仕様の"Set Watchdog Timer Command"の章を参照してください。
http://www.intel.com/design/servers/ipmi/

3.2 WDT 更新プログラムを/usr/sbin ディレクトリー配下にコピーしてください。

```
# install -p -m 755 ResetWDT /usr/sbin
```

3.3 下記の例を参考に、WDT 更新プログラムの起動スクリプトファイル(以降「WDT 起動スクリプト」という)を作成してください。

この例ではファイル名を「watchdog」とします。

```
----------------------------------------
#! /bin/sh
#
# chkconfig: - 27 46
# description: software watchdog
#
# Source function library.

### BEGIN INIT INFO
# Provides: watchdog
# Required-Start:
# Should-Start: ipmi
# Required-stop:
# Default-Start: 2 3 5
# Default-stop:
# Short-Description: watchdog
# Description: software watchdog
### END INIT INFO

prog=/usr/sbin/ResetWDT

case "$1" in
    start)
        echo -n "Starting watchdog daemon: "
        ${prog} &
        echo
        ;;
    *)
        echo "Usage: watchdog {start}"
        exit 1
        ;;
esac
----------------------------------------
```

「prog=」に WDT 更新プログラム(この例では ResetWDT)の格納パスを指定してください。

3.4 上記の WDT 起動スクリプトを install コマンドでコピーしてください。

```
# install -p -m 755 watchdog /etc/init.d
```

3.5 WDT 更新プログラムを自動起動できるように設定してください。

```
# chkconfig –-add watchdog
# chkconfig watchdog on
```

チェック

Windows OS 上で、上記のプログラムおよびスクリプトファイルを作成するときには、ご使用中の Linux に対応したコードに変換してください。

4. OS を再起動してください。再起動にてストール監視機能が有効となります。
   # reboot

■ストール監視機能を無効にする手順
root 権限のあるユーザーでログインして、設定をしてください。

1. WDT 更新プログラムを自動起動しないように設定してください。

2. OS を再起動してください。再起動にてストール監視機能が無効となります。

■ストール監視機能の関連モジュールを削除する手順
root 権限のあるユーザーでログインして、設定をしてください。

1. WDT 更新プログラムを自動起動しないように設定してください。

2. WDT 更新プログラムおよび WDT 起動スクリプトを削除してください。

3. OS を再起動してください。

2. コンフィグレーションツール

/opt/nec/esmpro_sa/tools 配下にコンフィグレーションツール(以降、本ツールと表記)を提供しています。

1. 本ツールを使用するには、ESMPRO/ServerAgent Ver.4.4 以降が動作している必要があります。
   必ず、ESMPRO/ServerAgent Ver.4.4 以降をインストールして、動作させてください。
2. 本ツールを使用するには、root 権限が必要です。
   必ず、root 権限のあるユーザーでログインしてください。
3. 本ツールは複数同時に使用することはできません。
   また、ESMPRO/ServerAgent のコントロールパネル(ESMagntconf, ESMamsadm)も起動しないでください。
4. 本ツールの設定を ESMPRO/ServerAgent に反映するため、以下のどちらかを実行してください。
   ・以下のコマンドを実行して、ESMPRO/ServerAgent 関連サービスを再起動します。
     # /opt/nec/esmpro_sa/bin/ESMRestart
   ・以下のコマンドを実行して、OS を再起動します。
     # reboot
5. 本ツールは、コマンドラインインターフェースを使用する特性により、シェルスクリプトから実行することも可能ですが、以下のような点に注意してください。
   ・1 行目には「#!/bin/bash」を記述する。
   ・ファイルの保存時には改行コードを Linux 改行コード (LF)とする。
   メモ帳などの Windows 標準のエディタでは、ファイル保存時に自動的に改行コードが Windows 改行コード (CR+LF) に変換されます。
   ・設定項目に日本語を使用する場合は、文字コードは OS に合わせ、euc や UTF-8 を使用する。

esmamset コマンド

コマンドラインインターフェースを使用して、ESMPRO/ServerAgent が使用するラック名や通報関連の情報を設定します。esmamset コマンドでは、以下を設定できます。

1. ラック名の設定 (ラックマウント機種のみ)
2. SNMP コミュニティー名の設定
3. 通報手段(SNMP)の有効/無効設定
4. 通報手段(SNMP)の通報先 IP アドレスの追加または削除
5. 通報手段(TCP_IP In-Band)の有効/無効設定
6. 通報手段(TCP_IP In-Band)の IP アドレスの追加または削除
7. 通報手段(TCP_IP In-Band)で使用するポート番号の設定
8. ESMPRO/ServerAgent からのシステムシャットダウン 有効/無効の設定

esmsysrep コマンド

コマンドラインインターフェースを使用して、ESMPRO/ServerAgent が監視する Syslog 監視対象イベントを設定します。esmsysrep コマンドでは、以下を設定できます。

1. Syslog 監視対象イベントの追加
2. Syslog 監視対象イベントの変更
3. Syslog 監視対象イベントの削除

2.1 esmamsetコマンド

機 能

コマンドラインインターフェースを使用して、ESMPRO/ServerAgent が使用するラック名や通報関連の情報を設定します。esmamset コマンドでは、以下を設定できます。

1. ラック名の設定 (ラックマウント機種のみ)
2. SNMP コミュニティー名の設定
3. 通報手段(SNMP)の有効/無効設定
4. 通報手段(SNMP)の通報先 IP アドレスの追加または削除
5. 通報手段(TCP_IP In-Band)の有効/無効設定
6. 通報手段(TCP_IP In-Band)の IP アドレスの追加または削除
7. 通報手段(TCP_IP In-Band)で使用するポート番号の設定
8. ESMPRO/ServerAgent からのシステムシャットダウン 有効/無効の設定

設 定

esmamset コマンドの使用方法は以下のとおりです。

\# cd /opt/nec/esmpro_sa/tools/

\# ./esmamset [OPTION]

```
Usage:
esmamset [-r <rackname>] [-c <community>]
         [-s ON|OFF] [-d <delip|ALLIP  …>] [-a <addip …>]
         [-t ON|OFF] [-i <ip>] [-p <port>]
         [-o ON|OFF]
         [-f <filename>]
         [-h]
```

[OPTION] 指定

[OPTION] には以下のオプションを指定します。複数のオプションを同時に指定することもできます。
設定する値にスペースが含まれるときは、前後に”(ダブルクォーテーション)を付加してください。

オプション	説明
-r <rackname>	ラック名を設定します。
-c <community>	コミュニティー名を設定します。 snmpd.conf に設定されていないコミュニティー名を指定したときは、設定は変更されませんので、先に snmpd.conf を修正してください。
-s ON|OFF	通報手段(SNMP)の有効/無効を設定します。 ON :有効 / OFF :無効
-d <delip ...>	通報手段(SNMP)に指定されている通報先 IP アドレスを削除します。 半角スペースを空け、2 つ以上の IP アドレスを同時に削除することもできます。
-d <ALLIP>	通報手段(SNMP)に指定されている通報先 IP アドレスを全て削除します。
-a <addip ...>	通報手段(SNMP)に指定されている通報先 IP アドレスを追加します。 半角スペースを空け、2 つ以上の IP アドレスを同時に追加することもできます。
-t ON|OFF	通報手段(TCP_IP In-Band)の有効/無効を設定します。 ON :有効 / OFF :無効

オプション	説明
-i <ip>	通報手段(TCP_IP In-Band)の通報先 IP アドレスを指定します。
-p <port>	通報手段(TCP_IP In-Band)で使用するポート番号を指定します。ファイアウォールを設定している場合は指定したポートを開放してください。
-o ON|OFF	ESMPRO/ServerAgent からのシステムシャットダウンの有効/無効を設定します。 ON :有効 / OFF :無効
-f <filename>	配置ファイルを指定して読み込み、ファイルに記載の内容に従って、各種設定をします。配置ファイルは後述します。 配置ファイルを読み込めた時点で、成功と判断するため、配置ファイル内で指定されたオプションが不正であっても戻り値は 0 (成功)を返却します。
-h	ヘルプ (Usage:)を表示します。

配置ファイル

[OPTION]で指定する内容が記載されたテキストファイルのことを指します。配置ファイルを -f オプションで指定して読み込むことで、[OPTION]を指定したときと同じことができます。
配置ファイルは
keyname "value"
の形式で記載します。keyname と ダブルクォート(")の間には空白(スペースかタブ)を入れてください。
また、改行コードが Linux 改行コード(LF)となるように注意してください。Windows 改行コード(CR+LF)で保存されたテキストファイルのときは、配置ファイルの内容を正しく読み込むことができません。
keyname の説明は下表を参照してください。

keyname(大文字)	説明
RACKNAME	-r オプションで指定する内容と同じです。
COMMUNITY	-c オプションで指定する内容と同じです。
SNMP	-s オプションで指定する内容と同じです。
DELIP	-d オプションで指定する内容と同じです。
ADDIP	-a オプションで指定する内容と同じです。
IN-BAND	-t オプションで指定する内容と同じです。
IN-BANDIP	-i オプションで指定する内容と同じです。
IN-BANDPORT	-p オプションで指定する内容と同じです。
SHUTDOWN	-o オプションで指定する内容と同じです。

戻り値

esmamset コマンドの戻り値は以下のとおりです。エラーメッセージはコンソールに表示しません。

戻り値	説明
0	設定に成功しました。
1	設定に失敗しました。指定されているオプションの内容を確認してください。
2	設定に失敗しました。ESMPRO/ServerAgent をインストールしてください。
4	設定に失敗しました。ログインしているユーザーにコマンドの実行権限がありません。

2.2 esmsysrepコマンド

機 能

コマンドラインインターフェースを使用して、ESMPRO/ServerAgent が監視する Syslog 監視対象イベントを設定します。esmsysrep コマンドでは、以下を設定できます。

1. Syslog 監視対象イベントの追加
2. Syslog 監視対象イベントの変更
3. Syslog 監視対象イベントの削除

設 定

esmsysrep コマンドの使用方法は以下のとおりです。

```
# cd /opt/nec/esmpro_sa/tools/
# ./esmsysrep [ACTION] [SOURCE] [EVENT] [OPTION]
```

```
Usage:
  esmsysrep --add -S <sourcename> -E <eventid> -K <keyword1> [OPTION]...
  esmsysrep --mod -S <sourcename> -E <eventid> [-K <keyword1>] [OPTION]...
  esmsysrep --del -S <sourcename> -E <eventid>
  esmsysrep --help

Action-selection option and specification:
--help    Show this help message
--add     Add an event id
--mod     Change the configuration of event id
--del     Delete an event id

Common option and specification:
-S <sourcename>     Specify the source name
-E <eventid>        Specify the event id
-K,-1 <keyword1>    Specify the first keyword, and the argument of
                    -K will be used if -1 and -K are both specified.
                    It can’t be omitted when --add is specified.

Other options(defaults in [ ] will be used if the options are not specified in --add):
-2 <keyword2>       Specify the second keyword. [ “” ]
-3 <keyword3>       Specify the third keyword. [ “” ]
-s <ON|OFF>         Set ON/OFF of the SNMP report method. [ ON ]
-i <ON|OFF>         Set ON/OFF of the TCP/IP IN-BAND report method. [ OFF]
-o <ON|OFF>         Set ON/OFF of the TCP/IP OUT-OF-BAND report method. [ OFF]
-t <trapname>       Set the trap name. [ “” ]
-d <dealmethod>     Set the deal method. [  “”  ]
-w <watchtime>      Set the watch time. [  “0-24”  ]
-c <reportcount>    Set the report count. [ 1 ]
-r <NONE|SHUTDOWN|REBOOT>    Set the action after a report. [ NONE ]
```

コマンド使用例

./esmsysrep --add -S TESTSOURCE -E 80001234 -K "test1234" -t "テスト通報"

上記の例では、
・ソース名 TESTSOURCE に、80001234 のイベント ID を新規追加します。
・ESMPRO/ServerAgent 関連サービスまたは OS の再起動後、syslog(/var/log/messages)に、文字列"test1234"が記録されると、Syslog 監視機能にて検出し、イベント ID:80001234 を SNMP で通報します。
・アラートビューアで表示するトラップ名は"テスト通報"となります。

[ACTION] 指定

[ACTION] には以下のオプションを指定します。省略することはできません。
また、複数のオプションを同時に指定することはできません。

オプション	説明
--add	Syslog イベントを追加します。
--mod	既存の Syslog イベントを変更します。
--del	Syslog イベントを削除します。
--help	ヘルプ (Usage:)を表示します。

[SOURCE] 指定

[SOURCE] には以下のオプションを指定します。省略することはできません。

オプション	説明
-S <sourcename>	[ACTION]の対象となるソース名を半角英数字の大文字で指定します。

[EVENT] 指定

[EVENT] には以下のオプションを指定します。省略することはできません。

オプション	説明
-E <eventid>	[ACTION]の対象となるイベント ID を 16 進数(0～F)の 8 桁で指定します。 イベント ID の上 4 桁は状態を表しますので、任意に指定できるのは、下 4 桁です。 C000nnnn 異常通報(赤色) 8000nnnn 警告通報(黄色) 4000nnnn 正常通報(緑色)

[OPTION] 指定

[OPTION] には以下のオプションを指定します。複数のオプションを同時に指定することもできます。
設定する値にスペースが含まれるときは、前後に"(ダブルクォーテーション)を付加してください。

オプション	説明
-K <keyword1> -1 <keyword1>	keyword1 を設定します。256 バイト以内の 1 バイト文字を使用します。-K と-1 を同時に指定したときは、-K の内容が設定されます。 [ACTION]が--add のときは省略することができません。
-2 <keyword2>	keyword2 を設定します。256 バイト以内の 1 バイト文字を使用します。 [ACTION]が--add のときの既定値は、""(空白)です。
-3 <keyword3>	keyword3 を設定します。256 バイト以内の 1 バイト文字を使用します。 [ACTION]が--add のときの既定値は、""(空白)です。
-s ON|OFF	通報手段(SNMP)の有効または無効を設定します。 ON : 有効 / OFF : 無効

オプション	説明
	[ACTION]が--add のときの既定値は、"ON"です。
-i ON|OFF	通報手段(TCP_IP In-Band)の有効または無効を設定します。 ON : 有効 / OFF : 無効 [ACTION]が--add のときの既定値は、"OFF"です。
-o ON|OFF	通報手段(TCP_IP Out-of-Band)の有効または無効を設定します。 ON : 有効 / OFF : 無効 [ACTION]が--add のときの既定値は、"OFF"です。
-t <trapname>	アラートビューアで表示するトラップ名を設定します。79 バイト以内の文字列で、1 バイトまたは 2 バイト文字が使用できます。日本語も使用できます。 [ACTION]が--add のときの既定値は、""(空白)です。
-d <dealmethod>	アラートビューアで表示する対処を設定します。507 バイト以内の文字列で、1 バイトまたは 2 バイト文字が使用できます。日本語も使用できます。 [ACTION]が--add のときの既定値は、""(空白)です。
-w <watchtime>	監視時間帯を設定します。複数の時間帯を指定するときは、カンマ(,)区切りで設定します。 [ACTION]が--add のときの既定値は、"0-24"です。
-c <reportcount>	監視時間帯における、通報に必要な該当イベントの発生回数を 1～65535 の数字で設定します。 [ACTION]が--add のときの既定値は、"1"です。
-r <NONE | SHUTDOWN | REBOOT>	通報後の動作を設定します。<action>は以下のいずれかを設定します。 NONE : 何もしない SHUTDOWN : シャットダウン REBOOT : 再起動 [ACTION]が--add のときの既定値は、"NONE"です。

戻り値

esmsysrep コマンドの戻り値は以下のとおりです。
戻り値が 0 以外のときは、コンソールにエラーメッセージを表示します。

戻り値	説明
0	設定に成功しました。
0 以外	設定に失敗しました。詳細はエラーメッセージを参照してください。

エラーメッセージ

エラーメッセージは以下のとおりです。

メッセージ	説明	戻り値
Only root can execute the tool.	ログインしているユーザーに実行権限がありません。	1
プログラム名: error while loading shared libraries: ライブラリーのパス: cannot open shared object file: No such file or directory	ESMPRO/ServerAgent がインストールされていません。	127
parameter error : "オプション名" is not specified.	省略不可の"オプション名"が指定されていません。	1
parameter error : argument of "オプション名" is too long.	"オプション名"に指定したパラメーターの文字列長が長すぎます。	1
parameter error : argument of "オプション名" is too short.	"オプション名"に指定したパラメーターの文字列長が短すぎます。	1
parameter error : argument of "オプショ	"オプション名"に指定したパラメーターは無効で	1

メッセージ	説明	戻り値
ン名" is invalid.	す。	
parameter error : option "オプション名" requires an argument.	"オプション名"にパラメーターが指定されていません。	1
parameter error : invalid option "オプション名".	"オプション名"に指定したオプションは無効です。	1
parameter error : "オプション名".	"オプション名"に指定したオプションが不正です。	1
Can't make all of the keywords empty.	--mod の設定を反映すると、キーワード(1～3)が、すべて""(空白)となります。	1
Can't access "<sourcename>", which isn't the object source of this tool.	本コマンドで設定できないイベント ID が指定されました。	1
ESMntserver service is not started.	ESMntserver が起動していません。	1
Other program is accessing the syslog events setting.	他のプログラム(ESMamsadm など)が syslog 設定にアクセスしているため、アクセスできません。	1
"<sourcename>/<eventid>" already exists.	--add で指定したソース名/イベント ID は、すでに存在しています。	1
"<sourcename>/<eventid>" doesn't exist.	--mod または –-del で指定したソース名/イベント ID は存在しません。	1
Access the "<sourcename>/<eventid>" failed.	[ACTION]に失敗しました。	1

ESMPRO/ServerAgent Ver. 4.5

5

注意事項

ESMPRO/ServerAgent の注意事項について説明します。

1. ESMPRO/ServerAgent

2. ESMPRO/ServerAgent for VMware

3. SUSE Linux Enterprise Server

4. Red Hat Enterprise Linux 5

「対象」に OS の Update や SP、バージョンを記載していないときは、Update や SP、バージョンに依存せず対象となります。

Linux サポート情報リストに、各ディストリビューションの注意・制限事項を公開しておりますので、こちらも参照してください。
■Linux サポート情報リスト【Linux サービスセットご契約のお客様限定】
https://www.support.nec.co.jp/View.aspx?id=3140001278

最新バージョンの ESMPRO/ServerAgent (Linux 版)は、次のウェブサイトからダウンロードできます。
予防保守の観点から最新バージョンの ESMPRO/ServerAgent (Linux 版)を、ご利用することをお勧めします。
https://www.express.nec.co.jp/linux/dload/esmpro/index.html
左側のメニューの「ESMPRO/ServerAgent」から「ソフトウェアのご使用条件」のご使用条件をご確認の上、「同意する」を選択します。
「ESMPRO/ServerAgent (Linux 版) ダウンロードページ」からご使用のディストリビューション(アーキテクチャー)を選択し、装置に合った物件を入手します。

最新バージョンの ESMPRO/ServerAgent for VMware は、次のウェブサイトからダウンロードできます。
■ESMPRO/ServerAgent for VMware サポート対象の追加物件
https://www.support.nec.co.jp/View.aspx?id=9010100940
※インストールには、ESMPRO/ServerAgent for VMware 製品メディアが必要です。

I. ESMPRO/ServerAgent

OS に依存しない、または複数の OS に関する注意事項です。

OS起動時に、ESMamvmainでsegfaultが発生するときがある

<更新> SA45_J-UG-L-010-01-003

対象：ESMPRO/ServerAgent Ver.4.5.6-1 未満

修正：ESMPRO/ServerAgent Ver.4.5.6-1

詳細：ESMamvmain サービスが起動する際に、OS システムコールである setenv と gethostbyname_r 内で使用される getenv の処理が競合して、getenv が不正なアドレスを参照するため、タイミングにより、segfault が発生します。
現象が発生した場合は、syslog に以下のメッセージが記録されます。
kernel: ESMamvmain[0000]: segfault at 0000000000000000 rip 0000000000000000 rsp 0000000000000000 error 4
※PID やアドレスを示す値は、状況により異なります。

対処：ESMPRO/ServerAgent Ver.4.5.6-1 以降に、アップグレードしてください。
お使いの環境向けに ESMPRO/ServerAgent Ver. 4.5.6-1 以降がリリースされていない場合は、回避策にて対処をお願いします。

回避：ESMamvmain を起動します。
/etc/rc.d/init.d/ESMamvmain start

温度・電圧・ファンの異常を検出できないときがある

<追加> SA45_J-UG-L-010-01-002

対象：ESMPRO/ServerAgent Ver.4.5.2-1 未満

修正：ESMPRO/ServerAgent Ver.4.5.2-1

詳細：温度・電圧・ファン異常を検出できず、以下の事象が発生する。
・本来であれば、ESMPRO/ServerManager のオペレーションウィンドウのアイコン色は異常(赤色)となるべきだが、警告(黄色)表示のまま変化しないため、本機本体ステータスランプと不一致が生じる。
・通報処理(エクスプレス通報やマネージャ通報、syslog へのメッセージ出力)が行われない。

対処：ESMPRO/ServerAgent Ver.4.5.2-1 以降に、アップグレードしてください。
お使いの環境向けに ESMPRO/ServerAgent Ver. 4.5.2-1 以降がリリースされていない場合は、回避策にて対処をお願いします。

回避：ESMPRO/ServerAgent 関連サービスを再起動します。
/opt/nec/esmpro_sa/bin/ESMRestart

参照：本件に関する情報は、次のウェブサイトに公開しております。
■【ESMPRO/ServerAgent(Linux)】温度・電圧・ファンの異常を検出できない場合がある
コンテンツ ID：9010102440
https://www.support.nec.co.jp/View.aspx?id=9010102440

OS起動時に、ESMamvmainでsegfaultが発生するときがある

<追加> SA45_J-UG-L-010-01-002

対象：ESMPRO/ServerAgent Ver.4.5.2-1 未満

修正：ESMPRO/ServerAgent Ver.4.5.2-1

詳細：ESMamvmain サービスが起動する際に実行する月 1 回の HeartBeat 通報とサービス起動毎の Syslog 監視スレッドの起動が競合して、不正なアドレスを参照するため、タイミングにより、segfault が発生します。
現象が発生した場合は、syslog に以下のメッセージが記録されます。
kernel: ESMamvmain[0000]: segfault at 0000000000000000 rip 0000000000000000 rsp

0000000000000000 error 4

※PID やアドレスを示す値は、状況により異なります。

対処：ESMPRO/ServerAgent Ver.4.5.2-1 以降に、アップグレードしてください。
お使いの環境向けに ESMPRO/ServerAgent Ver. 4.5.2-1 以降がリリースされていない場合は、回避策にて対処をお願いします。

回避：ESMamvmain を起動します。

/etc/rc.d/init.d/ESMamvmain start

ESMPRO/ServerAgentの仕様

アンマウントした時にファイルシステムの空き容量を誤検出するときがある
ESMfilesysのプロセスがCPU使用率100%となるときがある

対象：Linux OS

詳細：ファイルシステム監視機能は、監視間隔毎にマウントポイントを確認し、OS の関数である statfs()関数を利用して、ファイルシステム情報を取得しています。

1) マウントポイントを確認する。
2) マウントポイントを元に statfs()関数を利用して、情報を取得する。

上記の 1)と 2)の間にマウントポイントがアンマウントされたとき､statfs()関数からはエラーではなく、上位にあるマウントポイントのファイルシステム情報が返却される事を確認しました。

1) マウントポイントを確認(/hoge)する。
   →/hoge がアンマウントされる。
2) マウントポイント(/hoge)を元に statfs()関数を利用して、情報を取得する。
   空き容量/全容量は、上位である / の情報が返却される。

CLUSTERPRO を導入されているとき、クラスター構成システムでのクラスター停止時・フェイルオーバー発生時に本現象が発生する可能性があります。

対処：以下の 2 点あります。

ファイルシステム監視機能が新しいマウントポイントを検出したとき、既定値として、監視しないように変更することで、誤検出を防止します。コントロールパネルから監視する設定に変更できます。

<手順>

1) root 権限のあるユーザーでログインします。
2) 以下のコマンドでファイルシステム監視サービスを一時的に停止します。
   # /etc/rc.d/init.d/ESMfilesys stop
3) /opt/nec/esmpro_sa/data/ディレクトリーに移動します。
   # cd /opt/nec/esmpro_sa/data/
4) 念のため、ファイルシステム監視の設定ファイルをバックアップします。
   # cp esmfs.inf esmfs.org
5) vi コマンド等を使用して、esmfs.inf の 4 行目にある ThSwitchDef を以下のように変更します。
   [変更前] [変更後]
   ThSwitchDef=1 ThSwitchDef=0
6) 以下のコマンドでファイルシステム監視サービスを再開します。
   # /etc/rc.d/init.d/ESMfilesys start

アンマウント時に一時的にファイルシステム監視を停止します。

<手順>

1) root 権限のあるユーザーでログインします。
2) 以下のコマンドでファイルシステム監視サービスを一時的に停止します。
   # /etc/rc.d/init.d/ESMfilesys stop
3) ファイルシステムのアンマウントを実行します。
4) 以下のコマンドでファイルシステム監視サービスを再開します。

/etc/rc.d/init.d/ESMfilesys start

OSを再起動するとファイルシステム監視のしきい値が既定値となる

対象：ESMPRO/ServerAgent 全バージョン

詳細：ファイルシステム監視サービスが起動したときにマウントされていないマウントポイントは監視対象から外れるため、監視対象の設定を削除します。その後、マウントされて、マウントポイントを検出したときに新規マウントポイントと認識するため、監視対象の設定が既定値となります。

<システム起動後の動作例>

↓(オート)マウント[ポイント A]　→　システム起動前の設定を使用

↓ファイルシステム監視サービスの起動(マウントポイント確認)

マウント[ポイント A]を検出、設定は継続使用

マウント[ポイント B]は未検出、設定は削除(監視対象外とする)

↓(オート)マウント[ポイント B]

↓ファイルシステム監視サービスの監視間隔(マウントポイント確認)

マウント[ポイント B]を検出、設定は既定値(新規マウントポイントと認識)

回避：[前準備]

ファイルシステム監視サービス(ESMfilesys)を自動起動しない設定にします。

chkconfig ESMfilesys off

システムが起動して、すべてマウントした後にファイルシステム監視サービス(ESMfilesys)を起動します。

/etc/rc.d/init.d/ESMfilesys start

仮想化環境のホストOS上でESMPRO/ServerAgentを利用する

対象：仮想化しているホスト OS(VMware ESX, Red Hat Enterprise Linux KVM)

詳細：ESMPRO/ServerAgent は連続運用が危険な障害情報を検出したとき、デフォルトの設定ではシステムをシャットダウンします。仮想化環境でゲスト OS を稼動させている環境では、ゲスト OS がシャットダウンされずにサービスコンソールがシャットダウンするため、ゲスト OS からは予期せぬシャットダウンが発生したことになります。ゲスト OS の正常終了を重視されるときは、ESMPRO/ServerAgent からの通報によるシャットダウン機能を無効にして、障害発生時には手動で、ゲスト OS からシャットダウンしてください。

対処：[通報によるシャットダウン機能の設定手順]

1) root 権限のあるユーザーでログインします。
2) ESMamsadm が格納されているディレクトリーに移動します。
   # cd /opt/nec/esmpro_sa/bin/
3) コントロールパネル(ESMamsadm)を起動します。
   # ./ESMamsadm
4) コントロールパネル(ESMamsadm)の「通報基本設定」を選択します。
5) [通報基本設定]画面のその他の設定から「シャットダウン開始までの時間設定」を選択します。
6) 通報手段有効を無効('*'チェックを外す)にします。
7) 「OK」を選択します。

参照：本件に関する情報は、下記も参照してください。

■仮想化環境のホスト OS 上で ESMPRO/ServerAgent を利用する際の注意事項

コンテンツ ID：3150101496

https://www.support.nec.co.jp/View.aspx?id=3150101496

冗長電源縮退の通報ができないときがある

対象：ESMPRO/ServerAgent 全バージョン

詳細：OS 起動後に電源モジュールを追加して冗長電源構成としても、ESMPRO/ServerAgent 内部のデータが更新されないため、冗長電源縮退の通報はできません。

対処：以下のコマンドを実行して、ESMPRO/ServerAgent 関連サービスを再起動します。

/opt/nec/esmpro_sa/bin/ESMRestart

portmap (またはrpcbind)に関する注意事項

対象：Linux OS

詳細：ESMPRO/ServerAgent では、portmap (または rpcbind)の機能を利用しています。ESMPRO/ServerAgent 運用中に portmap (または rpcbind)の停止や再起動をされたとき、ESMPRO/ServerAgent は正常に動作できません。

対処：以下のコマンドを実行して、ESMPRO/ServerAgent 関連サービスを再起動します。

/opt/nec/esmpro_sa/bin/ESMRestart

シャットダウン時のsyslogにESMPRO/ServerAgentのメッセージが記録されるときがある

対象：ESMPRO/ServerAgent 全バージョン

詳細：シャットダウン時の syslog に以下のメッセージが記録されるときがあります。「XXXXX」は英数字で、状況により異なります。

###ERR###RPC###: RPC XXXXX

対処：シャットダウン時のみに発生する現象であり、次回 OS 起動時の動作に影響はありません。

シャットダウン時のsyslogにESMamvmainのメッセージが記録されるときがある

対象：64 ビット Linux OS 上で動作している ESMPRO/ServerAgent 全バージョン

詳細：シャットダウン時の syslog に以下のメッセージが記録されるときがあります。「XXXXX」は英数字で、状況により異なります。

kernel: ESMamvmain[XXXXX]: segfault at XXXXXXXXXXXXXXXX rip XXXXXXXXXXXXXXXX rsp XXXXXXXXXXXXXXXX error X

対処：シャットダウン時のみに呼び出している dlclose 関数内で発生する現象であり、次回 OS 起動時の動作に影響はありません。

システム高負荷時のsyslogにpidofのメッセージが記録されるときがある

対象：64 ビット Linux OS 上で動作している ESMPRO/ServerAgent 全バージョン

詳細：ESMPRO/ServerAgent では、pidof コマンドを使用する処理があり、システム高負荷時の syslog に以下のメッセージが記録されるときがあります。「XXXXX」は数字で、状況により異なります。

pidof[XXXXX]: can't read sid for pid XXXXX

対処：OS の動作、ESMPRO/ServerAgent の動作に影響はありません。

SNMP通報の遅延もしくはSNMP通報漏れが発生するときがある

対象：ESMPRO/ServerAgent 全バージョン

詳細：ESMPRO/ServerManager を起動した状態で、かつサーバ状態/構成情報の更新間隔をデフォルト設定(60 秒)より短く設定したとき、通報の遅延もしくは通報漏れが発生する事があります。

対処：サーバ状態/構成情報の更新間隔はデフォルト設定の 60 秒以上で運用するようにしてください。またはマネージャ通報(TCP/IP)を使用するように運用してください。

OS起動時のSNMP通報遅延が発生するときがある

対象：ESMPRO/ServerAgent 全バージョン

詳細：OS 起動時に通報の準備ができていない時に通報対象の現象が発生したとき、リトライ処理をします。通報対象の現象が発生するタイミングにより、OS 起動時に通報されるときとリトライ(5 分)後に通報されるときがあります。

対処：OS が起動してから 5 分以上経過後に、アラートビューアへ表示されるメッセージを確認してください。

SNMP通報の通報手段が有効でないときにもSNMP通報が送信されるときがある

対象：Linux OS

詳細：OS 起動時に通報の準備ができていない時に通報対象の現象が発生したとき、リトライ処理をします。

リトライ処理は、SNMP の通報手段(ON/OFF)に関係なく、通報を処理するため、リトライ処理をするタイミングで、トラップ通報先 IP が設定されたとき、SNMP 通報の通報手段が OFF のときでも通報します。

対処：通報させたくないとき、OS 起動後 5 分以上経ってから設定してください。

障害情報採取ツールを実行中にコンソールの表示またはsyslogにメッセージが記録されるときがある

対象：(例 1,2) net-snmp-5.3.1-24.el5

(例 3) net-snmp-5.5-44.el6 (Red Hat Enterprise Linux 6.4)

詳細：障害情報採取ツール(collectsa.sh)を実行中、コンソールの表示または syslog に以下のメッセージが記録されるときがあります。

例 1 : process 'sysctl' is using deprecated sysctl (syscall) net.ipv6.neigh.vswif0.base_reachable_time; Use net.ipv6.neigh.vswif0.base_reachable_time_ms instead.

例 2：process 'cp' is using deprecated sysctl (syscall) net.ipv6.neigh.vswif0.base_reachable_time; Use net.ipv6.neigh.vswif0.base_reachable_time_ms instead.

例 3：kernel: netlink: 12 bytes leftover after parsing attributes.

対処：OS の動作であり、対処はありませんが、ESMPRO/ServerAgent の動作に影響はありません。

EMカード搭載装置のラック名変更

対象：EM カード搭載装置

詳細：EM カード搭載のブレード収納ユニットに取り付けた CPU ブレードのときは、ESMPRO/ServerAgent のコントロールパネル(ESMagntconf)の[全般]画面から「Rack Name」を変更することはできません。

対処：Web コンソール機能等の EM カードの機能を使用して、設定してください。設定手順は、ブレード収納ユニットユーザーズガイドを参照してください。

WebSAM AlertManagerとの通報連携するためには、レジストリーを登録する

対象：ESMPRO/ServerAgent 全バージョン

詳細：Syslog イベントの設定で追加したイベントを WebSAM AlertManager で通報連携するとき、ESMPRO/ServerManager をインストールしたマシンに、以下のレジストリーを登録してください。

対処：レジストリーに以下のキー、名前、データを設定してください。

xxxx が新しく設定するアラートタイプの名前です。

アラートタイプ(xxxx)には以下を設定してください。

・Syslog 監視で設定した通報ソース名

Syslog 監視では、通報ソース名がアラートタイプに変換されるため。

・以下のアラートタイプ

AM

bootmsglogger

DS450

※64bit OS では、以下の記述の

HKEY_LOCAL_MACHINE¥SOFTWARE¥NEC

を

HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥NEC

に読み替えてください。

```
--------------------------------------------------------------------------
[HKEY_LOCAL_MACHINE¥SOFTWARE¥NEC¥NVBASE¥AlertViewer¥AlertType¥xxxx]
"WavDefault"="Server.wav"
"AniDefault"="Default.bmp"
"Image"="Default.bmp"
```

"SmallImage"="Default.bmp"

＝の左辺が名前、右辺がデータです。
データはいずれも文字列型です。

Windows XP(Home Edition は除く), 2000/2003, Vista では追加したアラートタイプのキー(~¥AlertType¥xxxx) に対して、以下のアクセス権を設定してください。

Administrators	フルコントロール
Everyone	読み取り
SYSTEM	フルコントロール
ESMPRO ユーザーグループ (*)	フルコントロール

(*) ESMPRO ユーザーグループ は、ESMPRO/ServerManager インストール時に指定した、ESMPRO を使用するユーザーを管理するためのグループ名です。
これはインストール時にユーザーが指定するグループ名ですが、以下のレジストリーにも格納されています。

[HKEY_LOCAL_MACHINE¥SOFTWARE¥NEC¥NVBASE]
名前：LocalGroup

以下の製品ページ FAQ もご参考にしてください。
http://www.nec.co.jp/middle/WebSAM/products/p_am/faq.html
Q43.アラートタイプの追加手順を教えてください。

ESMPRO/ServerManagerの表示

温度/電圧/ファンの状態が不明または現在値、回転数が表示されない

対象：奇数枚の DIMM を実装している装置
詳細：機種により、状態、現在値、回転数、しきい値などの情報を持たない温度/電圧/ファンのセンサーが存在します。そのため、ESMPRO/ServerManager で該当センサーを参照したときに、以下のように表示されることがありますので注意してください。
・ESMPRO/ServerManager の[サーバ状態/構成情報]で、状態が「不明」と表示される。
・ESMPRO/ServerManager の[サーバ状態/構成情報]で、現在値、回転数が表示されない。
または「不明」と表示される。
対処：対処はありませんが、表示のみの影響であり、ESMPRO/ServerAgent の監視に影響はありません。

奇数枚のDIMMを実装しているときに、メモリバンクが未実装(グレイ表示)となる

対象：奇数枚の DIMM を実装している装置
詳細：奇数枚の DIMM を実装しているときに、[構成情報]-[ハードウェア]-[メモリバンク]が未実装(グレイ表示)と表示されますが、実際に実装されているメモリと同じ実装位置が正常になっていれば問題ありません。DIMM の警告/異常が発生した場合には、メモリバンクが黄色(警告)/赤色(異常)になり、障害を検知することは可能です。
対処：対処はありませんが、表示のみの影響であり、ESMPRO/ServerAgent の機能に影響はありません。

ext4のファイルシステムが不明と表示されるときがある

対象：ファイルシステムに ext4 を利用している Linux OS
詳細：[構成情報]-[ファイルシステム]-[(監視対象デバイス名)]-[付加情報]のファイルシステムが不明と表示されます。ESMPRO/ServerAgent Ver.4.4.26-1 より、ファイルシステム ext4 をサポートしておりますが、ESMPRO/ServerManager が表示をサポートしていないためです。
対処：ESMPRO/ServerManager Ver.5.40 以降(Windows)を使用してください。

ハードディスクドライブ交換後にストレージが警告のままとなるときがある

対象：ESMPRO/ServerAgent 全バージョン

詳細：ハードディスクドライブの交換や追加したとき、 [構成情報]-[ストレージ]が正しく表示されないときがあります。

対処：構成タブをクリックし、構成情報を再度読み込んでください。また、ハードディスクドライブの交換や追加をしたときは、2 章の管理機能「5.ストレージ監視」を参照して、交換もしくは追加した監視対象ハードディスクドライブの情報をリセットしてください。

DVDコンボドライブを搭載した機種で、[構成情報]-[ストレージ]-[CD-ROM]を複数表示するときがある

対象：DVD コンボドライブを搭載した機種の 2.4 系カーネル以降

詳細：2.4 系カーネルでは、IDE 接続の書き込み可能な光ドライブの書き込み機能を使用するとき、ide-scsi エミュレーションが必要となるため、IDE 接続と SCSI 接続の両方から認識されるために本現象が発生します。

対処:対処はありませんが、表示のみの影響のみであり、ESMPRO/ServerAgent の機能に影響はありません。

ネットワークの転送スピードが正しく表示されないときがある

対象：Linux OS

詳細：ハードウェアの仕様、および、ドライバーの仕様により、[構成情報]-[ネットワーク]において、ネットワークの転送スピードが正しく表示されないときがあります。

対処：対処はありませんが、表示のみの影響であり、ESMPRO/ServerAgent の機能に影響はありません。

サポートしているネットワークのインタフェースタイプ

対象：Linux OS

詳細：ESMPRO/ServerManager がサポートしているネットワークのインタフェースタイプはイーサネット、ループバックのみとなります。それ以外のタイプのときは、ネットワークのタイプが正しく表示されないときがあります。

Nianticチップ(LOM/10G-KR Mezz等)のMAC情報

対象：Linux OS

詳細： [構成情報]-[ネットワーク]-[(ネットワークインターフェース名)]-[MAC 情報]は、net-snmp が作成する EtherLike-MIB の中のから取得しています。Niantic チップのドライバーには MAC 情報の一部の情報を取得する処理が実装されていないため、上記の EtherLike-MIB に MAC 情報の一部が存在しないため正しく表示されないときがあります。

対処：対処はありませんが、表示のみの影響であり、ESMPRO/ServerAgent の機能に影響はありません。

物理メモリ使用量の表示

対象：ESMPRO/ServerAgent 全バージョン

詳細：[構成情報]-[システム]-[メモリ]で表示している物理メモリ使用量は、/proc/meminfo の情報を元に以下の計算式で、メモリ使用率を算出しています。

メモリ使用量 = MemTotal-MemFree

上記値は、Buffers と Cached を含んだ値となるため、OS の状況によっては、高い値が表示されるときがあります。

システムの構成を正しく表示できないときがある

<更新> SA45_J-UG-L-010-01-003

対象：ESMPRO/ServerAgent Ver.4.5.0-1 未満

改善：ESMPRO/ServerAgent Ver.4.5.0-1 以降

詳細：ESMPRO/ServerManager を起動した状態で、ホットスワップに対応したファンを抜いたとき、構成情報を正しく表示できないときがあります。

対処：処理を改善した ESMPRO/ServerAgent Ver.4.5.0-1 以降にアップグレードするか、システムの構成を変更したときは、5 分程待機した後に構成タブをクリックし、構成情報を再度読み込んでください。

シリアルポートのコネクタ形状が不明と表示されるときがある

対象：SMBIOS Type8 Port Connector Information が未サポートの装置

詳細：[構成情報]-[I/O デバイス]で表示しているシリアルポートのコネクタ形状は、SMBIOS Type8 Port Connector Information の情報を元に表示しております。SMBIOS Type8 Port Connector Information が未サポートの装置において、シリアルポートのコネクタ形状は、不明と表示します。SMBIOS Type8 のサポート有無は、dmidecode コマンドの実行結果に以下の情報(type 8)が表示されるかを確認してください。

Handle 0x000C, DMI type 8, 9 bytes
Port Connector Information

対処：対処はありませんが、表示のみの影響であり、ESMPRO/ServerAgent の機能に影響はありません。

マウス情報が表示されない

対象：VMware ESX 4, SUSE Linux Enterprise Server, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 5, Asianux Server 3, MIRACLE LINUX V4.0

詳細：[構成情報]-[I/O デバイス]で表示しているマウス情報は、/etc/sysconfig/mouse ファイルの内容を情報元としています。そのため、/etc/sysconfig/mouse ファイルが存在しないとき、マウス情報は表示されません。

対処：対処はありませんが、表示のみの影響であり、ESMPRO/ServerAgent の監視機能に影響はありません。

ディスプレイアダプター情報の垂直解像度と水平解像度、ピクセルが 0 で表示される

対象：Linux OS

詳細：[構成情報]-[I/O デバイス]で表示しているディスプレイアダプター情報の垂直解像度と水平解像度、ピクセルが 0 と表示されます。X-Windows をサポートしている OS は、X-Windows(仮想コンソールが /dev/tty7 のみ)にログインしたとき、垂直解像度と水平解像度、ピクセルを表示します。

垂直解像度 ：0 ピクセル、水平解像度 ：0 ピクセル、ピクセル ：0 ビット/ピクセル

対処：対処はありませんが、表示のみの影響であり、ESMPRO/ServerAgent の監視機能に影響はありません。

ハードディスクドライブ情報の表示

対象：Linux OS

詳細：[構成情報]-[ストレージ]で表示しているハードディスクドライブ情報は、/proc/scsi/scsi の情報を元にしており、実際のハードウェアと異なる情報が表示されるときがあります。一例として、SCSI ディスクや RAID 環境のときはデバイスから取得した値(INQUIRY)がそのまま Vendor に設定されますが、SATA ディスクのとき、T10 SCSI/ATA translation の仕様に従い、'ATA 'という文字列が入ります。

```
----
Host: scsi0 Channel: 00 Id: 00 Lun: 00
  Vendor: ATA      Model: SSDSA2SH064G1GC   Rev: 445C
  Type:   Direct-Access                     ANSI SCSI revision: 05
```

OS環境により、UUID/GUIDが異なるときがある

対象：Linux OS

詳細：[サーバ状態]で表示している GUID は、dmidecode コマンドより、[構成情報]-[ハードウェア]-[装置情報]-[システムマネージメント]の UUID/GUID は、SMBIOS から情報を取得しています。dmidecode のバージョンが 2.10 以降のときは、SMBIOS のバージョンを判断しています。SMBIOS のバージョンが 2.6 以降のときは UUID をバイトオーダーへ入れ替える処理があります。その影響により、UUID/GUID が異なるときがあります。

例)SMBIOS Ver.2.6 の値

12345678 ABCD EFGH IJKL MNOPQRSTUVWX

波下線の部分が 4byte 2byte 2byte 単位でバイト交換される。

78563412 CDAB GHEF IJKL MNOPQRSTUVWX

対処：ESMPRO/ServerManager Ver.5.28 以降を使用すれば、マネージメントコントローラ管理と SNMP 管理の両方が有効の場合は、別々のサーバーとして登録される問題が修正されています。

スケーラブルHAサーバーの注意事項

OS起動後に状態色が反映されるまでに15分程度かかるときがある

対象：Express5800/A1040, A1040a, A1160, A1080a

詳細：OS 起動後、ESMPRO/ServerManager へ状態色が反映されるまでに 15 分程度かかるときがあります。状態色が反映されるまで、構成情報は正しく取得できません。センサーの種類によって、情報を取得に時間が掛かることがあり、装置に実装されているセンサー数により、時間が掛かります。

対処：ESMPRO/ ServerManager へ状態色が反映されるまで、お待ちください。

特定条件下において、サーバーの構成情報、稼働状況が表示できなくなるときがある

対象：Express5800/A1040a, A1080a に対して、
ESMPRO/ServerManager Ver.4 または Ver.5 Windows GUI を使用しているとき。

詳細：[構成情報]-[システム環境]配下にある情報を選択(表示)したとき、オペレーションウィンドウとサーバ状態/構成情報がグレー表示になり、サーバーの構成情報や稼働状況が表示できなくなり、サーバアクセス不能のアラートが登録されることがあります。サーバ状態/構成情報からセンサー情報を選択することにより、定期的な状態取得とタイミングが重なるときがあり。OpenIPMI ドライバー経由でのアクセス時に競合が発生し、タイムアウトが発生する可能性が高くなる事が原因です。

回避：ESMPRO/ServerManager Ver.5.31 未満を使用するときは、オペレーションウィンドウのメニューにある「オプション」-「カスタマイズ」-「動作環境」-「SNMP/ICMP パケット」-「再送間隔」にある既定値の"4 4 4 4"を"10 10 10 10"に変更してください。また、環境によっては、上記設定でもサーバアクセス不能が発生するときは、設定する値を大きくしてください。

対処：ESMPRO/ServerManager Ver.5.31 以降 (Windows)では、サーバー監視(サーバアクセス不能検出)を強化しておりますので、ESMPRO/ServerManager Ver.5.31 以降 (Windows) WEBGUI を使用してください。

2. ESMPRO/ServerAgent for VMware

ESMPRO/ServerAgent for VMware の注意事項です。
「対象」に Update やバージョンを記載していないときは、Update やバージョンに依存せず対象となります。

ESMPRO/ServerAgentの仕様

RDM(Raw Device Mapping)の設定が失敗するときがある

対象：VMware ESX 3, VMware ESX 4
詳細：ハードディスクドライブ単体構成のストレージ監視機能はサポートしていません。装置構成によりストレージ監視サービスが動作して、RDM(Raw Device Mapping)の設定が失敗するときがあります。
ESMPRO/ServerAgent for VMware インストレーションガイドの 3 章(3.1. インストール)にある手順 5)にて、以下のコマンドを実行したときは問題ありません。
sh /(マウントポイント)/esmpro_sa/vmset.sh -sata
対処：以下の手順で、ESMstrg サービスを起動しないように設定します。
ESMstrg サービスを停止します。
/etc/init.d/ESMstrg stop
ESMstrg サービスが自動起動しないように設定します。
/sbin/chkconfig ESMstrg off
ESMstrg のランレベルがすべての off であることを確認します。
/sbin/chkconfig --list ESMstrg
ESMstrg 0:off 1:off 2:off 3:off 4:off 5:off 6:off
参照：本件に関する情報は、次のウェブサイトにも公開しております。
■ESMPRO/ServerAgent for VMware ストレージ監視機能について
【PPSupportPack(ESMPRO/ServerAgent for VMware)ご契約のお客様限定】
コンテンツ ID：3140100091
https://www.support.nec.co.jp/View.aspx?id=3140100091

OSに含まれるパッケージの仕様

net-snmpの特定のAPIを使用すると、メモリリークが発生する

対象：VMware ESX 4.0 に含まれる net-snmp-5.3.1-24.el5_2.2
詳細：net-snmp の以下の API を使用すると、メモリを解放していないパスがあり、メモリリークが発生する。
・snmp_sess_init
・snmp_open
ESMPRO/ServerAgent(ESMcmn)サービスでは、net-snmp の API を使用する処理があるため、メモリリークが発生します。ESMPRO/ServerManager のローカルポーリング機能を利用したとき、1 ヶ月で約 2.6MB 程度のメモリリークが発生します。
対処：VMware ESX 4.0 に含まれる net-snmp のバージョンで発生する問題です。VMware ESX 4.0 Update 1 では修正されており、VMware より公開されているパッチを適用してください。
VMware ESX 4.0, Patch ESX400-Update01a :
http://kb.vmware.com/kb/1014842
VMware ESX 4.0, Patch ESX400-200911236-UG: Updates SNMP :
http://kb.vmware.com/kb/1014853

dlopen, dlclose関数を使用すると、少量のメモリリークが発生するときがある

対象：VMware ESX 4 に含まれる glibc-2.5-42 未満
修正：Red Hat Enterprise Linux 5 では、glibc-2.5-42 にて修正されております。

詳細 : dlopen, dlclose 関数で 1 回につき 16 バイト程度のメモリリークが発生します。ESMPRO/ServerAgent では、エクスプレス通報時に上記関数を使用していますが、エクスプレス通報 1 回あたりのメモリリーク量は 16Bytes であり、かつ、本通報は、ハードウェア障害が発生したときのみであり、頻発する通報ではありません。

対処 : VMware ESX 4 に含まれる glibc の不具合です。問題が修正された glibc パッケージが公開された際にはアップデートしてください。
dlopen, dlclose 関数を使用するアプリケーションの終了によりメモリは開放されます。
アプリケーションのメモリ使用量を確認し、適宜 ESMPRO/ServerAgent 関連サービスを再起動します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

ESMPRO/ServerManagerの表示

Express5800/A1080aに表示されるハードディスクドライブ情報

対象 : VMware ESX 4 が動作している Express5800/A1080a

詳細 : 装置内部に実装されている USB Flash Memory をハードディスクドライブと認識しますが、監視対象外であるため、ストレージ監視しません。
[表示例]
ハードディスク 一般情報

選択項目	:	[1] HAGIWARA bNAND2 Memory
容量	:	952 MB
シリンダ数/ユニット	:	1,015
トラック数/シリンダ	:	31
セクタ数/トラック	:	62
予防保守状態	:	予防保守を行っていません

Express5800/A1040, A1160に表示される「AMI Virtual Floppy」

対象 : VMware ESX 4 が動作している Express5800/A1040, A1160

詳細 : RemoteKVM で仮想 FD を接続するためのデバイスです。AMI Virtual Floppy というデバイスをハードディスクドライブと認識しますが、監視対象外であるため、ストレージ監視はしません。
[表示例]
ハードディスク 一般情報

選択項目	:	[1] AMI Virtual Floppy
容量	:	0 MB
シリンダ数/ユニット	:	0
トラック数/シリンダ	:	0
セクタ数/トラック	:	0
予防保守状態	:	予防保守を行っていません

[構成情報]-[ストレージ]-[コントローラ]配下の[IDE Controller]情報が表示されない

対象 : VMware ESX 4

詳細 : ESMPRO/ServerAgent は、ストレージの IDE デバイス情報として、/proc/ide ファイルを参照していますが、VMware ESX 4 では、/proc/ide ファイルが未サポートのため、表示されません。

ストレージ情報の表示が重複する

対象 : VMware ESX 4

詳細 : VMware ESX 4 では、USB 接続のデバイスを動的に取り扱えないため、デバイスの抜き差しを繰り返したとき、ストレージ情報が増加します。ESMPRO/ServerAgent は、/proc/scsi/scsi ファイルを参照していますが、OS の問題により本現象が発生します。

対処 : ゲスト OS から光ドライブを使用するときに影響があるため、「クライアントデバイス」、もしくは「データストア ISO ファイル」を利用してください。

論理CPU情報とメモリ量の表示

対象：VMware ESX 4

詳細：ESMPRO/ServerManager で表示している論理 CPU 情報とメモリ量(使用量/総容量)は、装置が持つ全体の値ではなく、サービスコンソールに割り当てられた値になります。

3. SUSE Linux Enterprise Server

SUSE Linux Enterprise Server に関する注意事項です。
「対象」に OS の SP やバージョンを記載していないときは、SP やバージョンに依存せず対象となります。

kernel-2.6.32.54-0.3.1において、ESMPRO/ServerManagerがグレー表示になるときがあります。

対象：Express5800/A1040a, A1080a に対して、kernel-2.6.32.54-0.3.1 を適用するとき。
詳細：SUSE Linux Enterprise Server 11 SP1 向けの kernel-2.6.32.54-0.3.1 は ipmi に関する以下の修正があります。

Description
The following non-security issues have been fixed:
・ipmi: reduce polling when interrupts are available (bnc#740867).
・ipmi: reduce polling (bnc#740867).

この修正により、[構成情報]-[システム環境]配下にある情報を選択(表示)したときの動作に影響があり、オペレーションウィンドウとサーバ状態/構成情報がグレー表示になり、サーバーの構成情報や稼働状況が表示できなくなり、サーバアクセス不能のアラートが登録されることがあります。
対処：ESMPRO/ServerManager Ver.5.50 以降 (Windows) WEBGUI を使用してください。
■ESMPRO/ServerManager Ver. 5.50 (Windows)
コンテンツ ID：9010101231
https://www.support.nec.co.jp/View.aspx?id=9010101231
参照：Linux kernel 5732 (Novell ウェブサイト)
http://download.novell.com/Download?buildid=pXjJAHc77X4~

ESMPRO/ServerAgentの仕様

syslogローテート後のファイルが監視対象になりません

対象：SUSE Linux Enterprise Server
詳細：syslog ローテート後のファイルは/etc/logrotate.d/syslog に"compress"(圧縮する)が定義されており、Syslog 監視では、ローテート後のファイル名は圧縮された bzip2 ファイルとなり監視対象になりません。
そのため、syslog がバックアップされたタイミングで、通報漏れが発生する可能性がある。

```
messages           -------------------+
                                      | ←syslog のバックアップ
messages-年月日.bz2                    +---------------------------
                                 ***** ←監視できない
Syslog 監視(監視間隔) --------+--------+--------+--------
```

対処：/etc/logrotate.d/syslog の設定から、/var/log/messages は圧縮しない設定にします。

<修正前>	<修正後>
/var/log/warn	/var/log/warn
/var/log/messages	
/var/log/allmessages	/var/log/allmessages
/var/log/localmessages	/var/log/localmessages
/var/log/firewall	/var/log/firewall
/var/log/acpid	/var/log/acpid
/var/log/NetworkManager {	/var/log/NetworkManager {
compress	compress
dateext	dateext
(以下省略)	(以下省略)

/var/log/messages {
dateext
(以下省略)

OS起動時にESMpowsw関連のメッセージがsyslogへ記録されるときがある

対象：SUSE Linux Enterprise Server

詳細：OS 起動時の syslog に以下のメッセージが記録されるときがあります。

ESMpowsw: ###ERR###RPC###: RPC: Port mapper failure - RPC: Success

SUSE Linux Enterprise Server では、サービスの起動は複数同時に起動されるため、ESMPRO/ServerAgent の基幹サービスである ESMntserver サービスまたは OpenIPMI の起動が完了する前に ESMpowsw サービスが起動して、内部処理をしたときに記録されます。

対処：対処はありませんが、ESMPRO/ServerAgent の監視機能に影響はありません。

OS起動時に検出した事象が通報されない

対象：SUSE Linux Enterprise Server

詳細：ESMPRO/ServerAgent の Syslog 監視機能は、/var/log/messages のみが監視対象であり、/var/log/boot.msg に出力されたログは監視できないため、通報連携しているソフトウェアが OS 起動時に検出した事象を検出できません。

対処：以下の手順で boot.klogd サービスを停止することで、OS 起動時のログが/var/log/messages に出力されるようになり、通報連携しているソフトウェアが OS 起動時に検出した事象を ESMPRO/ServerAgent から通報できるようになります。

#insserv -r boot.crypto
#insserv -r boot.klog

OSに含まれるパッケージの仕様

net-snmpの特定のAPIを使用すると、メモリリークが発生する

対象：SUSE Linux Enterprise Server 10 SP3

詳細：net-snmp の以下の API を使用すると、メモリを解放していないパスがあり、メモリリークが発生する。

・snmp_sess_init
・snmp_open

ESMPRO/ServerAgent(ESMcmn)サービスでは、net-snmp の API を使用する処理があるため、メモリリークが発生します。

対処：問題が修正された net-snmp パッケージが公開されておりますので、次のウェブサイト(Novell ウェブサイト)よりダウンロードし、パッケージの適用をしてください。

・x86　：http://download.novell.com/Download?buildid=5VLiHe1PqvY~
・x86_64：http://download.novell.com/Download?buildid=Jg9Eta1qxts~

4. Red Hat Enterprise Linux 5

Red Hat Enterprise Linux 5 に関する注意事項です。

ESMPRO/ServerAgentの仕様

OS起動時にnet-snmp関連のメッセージがsyslogへ記録されるときがある

対象：Red Hat Enterprise Linux 5

詳細：OS 起動時に以下のメッセージが syslog へ記録されるときがあります。

snmpd[3384]: error finding row index in _ifXTable_container_row_restore

ESMPRO/ServerAgent 関連のサービスを起動し、かつファイアウォールを無効としたときに発生するときがあります。

対処：ESMPRO/ServerAgent 関連サービス起動時に net-snmp が IPV6 関連の処理を実行しようとしますが、IPV6 が設定されていないためにメッセージが記録されています。ESMPRO/ServerAgent では IPV6 関連の機能は使用しておらず、動作に影響はありません。

IPV6 を使用する設定を追加することで、メッセージは出力されなくなります。メッセージを出力されないよう設定するときは、/etc/sysconfig/network に NETWORKING_IPV6=yes を追加します。

参照：本件に関する情報は、下記の Red Hat Enterprise Linux 5 の注意・制限事項も参照してください。

■[RHEL5]注意・制限事項　ID:05082

https://www.support.nec.co.jp/View.aspx?id=3140001230

OSに含まれるパッケージの仕様

syslogにsnmpd関連のログが多数記録されるときがある

対象：net-snmp-5.1.2-11.EL4.10 以降

詳細：ESMPRO/ServerAgent は SNMP を利用しているため、net-snmp は syslog(/var/log/messages)へ以下のようなログが多数記録されるときがあります。

snmpd[5824]: Connection from - 127.0.0.1
snmpd[5824]: transport socket = 12
snmpd[5824]: Received SNMP packet(s) from UDP: [127.0.0.1]:7023

net-snmp-5.1.2-11.EL4.10 以降は、INFO レベルでログが出力されるためです。

対処：既定値では INFO レベルでログを出力されていますが、オプションを指定することにより、NOTICE レベル以上のログのみを出力するように制限できます。

・net-snmp-5.3.2.2-5.el5 未満

<設定方法>

1. /etc/snmp/snmpd.options に以下を設定後、snmpd サービスを再起動します。
   OPTIONS=”-LS e d -Lf /dev/null -p /var/run/snmpd.pid –a”

・net-snmp-5.3.2.2-5.el5 以降

<設定方法>

1. /etc/snmp/snmpd.conf に以下を設定します。
   dontLogTCPWrappersConnects yes
2. /etc/sysconfig/snmpd.options に以下を設定後、snmpd サービスを再起動します。
   OPTIONS="-Lsd -Lf /dev/null -p /var/run/snmpd.pid"

参照：本件に関する情報は、下記も参照してください。

■Red Hat Knowledgebase: snmpd から過剰に出力されるログを制限する方法を教えてください。

https://access.redhat.com/knowledge/ja/articles/14859

(Subscriber content preview. For full access to the Red Hat Knowledgebase)

RHEL5.1/5.2/5.3に含まれるdlopen, dlclose関数で少量のメモリリークが発生する

対象：Red Hat Enterprise Linux 5.1, 5.2, 5.3

修正：glibc-2.5-42 以降

詳細：dlopen, dlclose 関数で 1 回につき 16 バイト程度のメモリリークが発生します。ESMPRO/ServerAgent では、エクスプレス通報時に上記関数を使用していますが、エクスプレス通報 1 回あたりのメモリリーク量は 16Bytes であり、かつ、本通報は、ハードウェア障害が発生したときのみであり、頻発する通報ではありません。

対処：Red Hat Enterprise Linux 5.1, 5.2, 5.3 に含まれる glibc の不具合です。問題が修正されたパッケージにアップデートしてください。RHN(Red Hat Network)より、glibc-2.5-42 以降のパッケージをダウンロードし、インストール済みのパッケージに対して、適用してください。

・x86
glibc-2.5-42.i386.rpm
glibc-2.5-42.i686.rpm
glibc-common-2.5-42.i386.rpm
glibc-devel-2.5-42.i386.rpm
glibc-headers-2.5-42.i386.rpm
glibc-utils-2.5-42.i386.rpm
nscd-2.5-42.i386.rpm

・EM64T
glibc-2.5-42.i686.rpm
glibc-2.5-42.x86_64.rpm
glibc-common-2.5-42.x86_64.rpm
glibc-devel-2.5-42.i386.rpm
glibc-devel-2.5-42.x86_64.rpm
glibc-headers-2.5-42.x86_64.rpm
glibc-utils-2.5-42.x86_64.rpm
nscd-2.5-42.x86_64.rpm

参照：本修正に関する情報は、下記の Red Hat Enterprise Linux 5 の注意・制限事項も参照してください。
■[RHEL5]注意・制限事項　ID:05143
https://www.support.nec.co.jp/View.aspx?id=3140001230

RHEL5.2に含まれるnet-snmpの特定のAPIを使用すると、メモリリークが発生する

対象：Red Hat Enterprise Linux 5.2

回避：net-snmp-5.3.1-19.el5_1.4

詳細：net-snmp の以下の API を使用すると、メモリを解放していないパスがあり、メモリリークが発生する。
・snmp_sess_init
・snmp_open
ESMPRO/ServerAgent(ESMcmn)サービスでは、net-snmp の API を使用する処理があるため、メモリリークが発生します。

対処：Red Hat Enterprise Linux 5.2 に含まれる net-snmp のバージョンで発生するデグレードです。問題が発生しない net-snmp パッケージに戻すことで、問題を回避できます。RHN(Red Hat Network)より、net-snmp-5.3.1-19.el5_1.4 のパッケージをダウンロードし、インストール済みのパッケージに対して、適用してください。

・x86
net-snmp-5.3.1-19.el5_1.4.i386.rpm
net-snmp-devel-5.3.1-19.el5_1.4.i386.rpm
net-snmp-libs-5.3.1-19.el5_1.4.i386.rpm
net-snmp-utils-5.3.1-19.el5_1.4.i386.rpm

・EM64T
net-snmp-5.3.1-19.el5_1.4.x86_64.rpm
net-snmp-devel-5.3.1-19.el5_1.4.i386.rpm
net-snmp-devel-5.3.1-19.el5_1.4.x86_64.rpm
net-snmp-libs-5.3.1-19.el5_1.4.i386.rpm
net-snmp-libs-5.3.1-19.el5_1.4.x86_64.rpm
net-snmp-utils-5.3.1-19.el5_1.4.x86_64.rpm

バージョンを戻すことになるため、適用の際は以下のオプション指定で rpm コマンドを実行してください。

rpm -Uvh --oldpackage *.rpm

本件は、RHEL5.3 に含まれる net-snmp-5.3.2.2-5.el5 で修正されていますが、別の問題が発生することが確認されています。net-snmp パッケージに関する情報は、「RHEL5.3 に含まれる net-snmp サービスでメモリリークが発生するときがあります。」にも記載していますので、参照してください。
RHEL5.3 以降にアップデートしない OS では、問題の発生しない net-snmp-5.3.1-19.el5_1.4 にダウングレードすることで問題を回避してください。

参照：本修正に関する情報は、下記の Red Hat Enterprise Linux 5 の注意・制限事項も参照してください。

■[RHEL5]注意・制限事項　ID:05127
https://www.support.nec.co.jp/View.aspx?id=3140001230

RHEL5.3に含まれるnet-snmpサービスでメモリリークが発生する

対象：Red Hat Enterprise Linux 5.3
修正：net-snmp-5.3.2.2-5.el5_3.1 以降
詳細：ESMPRO/ServerAgent を稼動させたとき、1 時間に 70Kbyte 程度のメモリリークが発生するときがあります。
対処：Red Hat Enterprise Linux 5.3 に含まれる net-snmp のバージョンで発生するデグレードです。問題が修正された net-snmp パッケージにアップデートしてください。RHN(Red Hat Network)より、net-snmp-5.3.2.2-5.el5_3.1 以降にアップデートしてください。以下のパッケージを RHN(Red Hat Network)よりダウンロードし、インストール済みのパッケージに対して、適用してください。

・x86
net-snmp-5.3.2.2-5.el5_3.1.i386.rpm
net-snmp-devel-5.3.2.2-5.el5_3.1.i386.rpm
net-snmp-libs-5.3.2.2-5.el5_3.1.i386.rpm
net-snmp-perl-5.3.2.2-5.el5_3.1.i386.rpm
net-snmp-utils-5.3.2.2-5.el5_3.1.i386.rpm

・EM64T
net-snmp-5.3.2.2-5.el5_3.1.x86_64.rpm
net-snmp-devel-5.3.2.2-5.el5_3.1.i386.rpm
net-snmp-devel-5.3.2.2-5.el5_3.1.x86_64.rpm
net-snmp-libs-5.3.2.2-5.el5_3.1.i386.rpm
net-snmp-libs-5.3.2.2-5.el5_3.1.x86_64.rpm
net-snmp-perl-5.3.2.2-5.el5_3.1.x86_64.rpm
net-snmp-utils-5.3.2.2-5.el5_3.1.x86_64.rpm

RHEL5.4 に含まれる net-snmp-5.3.2.2-7.el5 で修正されていますが、別の問題が発生することが確認されています。net-snmp パッケージに関する情報は、「RHEL5.4 に含まれる net-snmp サービスでメモリリークが発生するときがあります。」にも記載していますので、参照してください。RHEL5.4 以降にアップデートをしない OS では、問題の発生しない net-snmp-5.3.2.2-5.el5_3.1 以降にアップデートすることで問題を回避してください。

参照：本修正に関する情報は、下記の Red Hat Enterprise Linux 5 の注意・制限事項も参照してください。
■[RHEL5]注意・制限事項　ID:05173
https://www.support.nec.co.jp/View.aspx?id=3140001230

RHEL5.4に含まれるnet-snmpサービスでメモリリークが発生する

対象：Red Hat Enterprise Linux 5.4
修正：net-snmp-5.3.2.2-9.el5 以降
詳細：ESMPRO/ServerAgent を稼動させたとき、1 時間に 80Kbyte 程度のメモリリークが発生するときがあります。Red Hat Enterprise Linux 5.3 で類似の問題(ID:05173)が発生し、net-snmp パッケージの修正で対応されていますが、本現象は Red Hat Enterprise Linux 5.3 の問題とは異なる原因で発生しているものと考えられます。
対処：net-snmp のサービスプログラム snmpd のメモリリークであり、リークしたメモリは使用されないため、他のプロセスのメモリ使用状況や時間経過によってスワップ領域に退避されるため、実メモリの使用には影響はありません。また、snmpd サービスを再起動することで、リークしたメモリを開放できます。snmpd のメモリ使用量を減らしたいときは、snmpd サービスを再起動してください。問題が修正された net-snmp-5.3.2.2-9.el5 以降にアップデートしてください。以下のパッケージを RHN(Red Hat Network)よりダウンロードし、インストール済みのパッケージに対して、適用してください。

・x86
net-snmp-5.3.2.2-9.el5.i386.rpm
net-snmp-devel-5.3.2.2-9.el5.i386.rpm
net-snmp-libs-5.3.2.2-9.el5.i386.rpm
net-snmp-perl-5.3.2.2-9.el5.i386.rpm
net-snmp-utils-5.3.2.2-9.el5.i386.rpm

・EM64T
net-snmp-5.3.2.2-9.el5.x86_64.rpm
net-snmp-devel-5.3.2.2-9.el5.i386.rpm
net-snmp-devel-5.3.2.2-9.el5.x86_64.rpm
net-snmp-libs-5.3.2.2-9.el5.i386.rpm
net-snmp-libs-5.3.2.2-9.el5.x86_64.rpm
net-snmp-perl-5.3.2.2-9.el5.x86_64.rpm
net-snmp-utils-5.3.2.2-9.el5.x86_64.rpm

参照：本修正に関する情報は、下記の Red Hat Enterprise Linux 5 の注意・制限事項も参照してください。

■[RHEL5]注意・制限事項　ID:05187
https://www.support.nec.co.jp/View.aspx?id=3140001230

syslogにsnmpd関連のメッセージが記録され、サーバ状態/構成情報が表示できないときがある

対象：Red Hat Enterprise Linux 5
修正：net-snmp-5.3.2.2-9.el5_5.1 以降 (Red Hat Enterprise Linux 5.6)
詳細：本現象は、net-snmp に含まれる snmpd に不具合があり、snmpd が MIB データを検索する処理にて、定期的にファイルのクローズが漏れることに起因します。この影響で、1 プロセスでオープンできるファイル記述子を使い切ってしまったため、新たに通信ソケットを生成できず、ESMPRO/ServerManager に関する通信ができなくなる可能性があります。
snmpd[5824]: could not open netlink socket
snmpd[5824]: couldn't create socket
対処：net-snmp のサービスプログラム snmpd が MIB データを検索する処理にて、定期的にファイルのクローズが漏れる不具合がありました。問題が修正された net-snmp-5.3.2.2-9.el5_5.1 以降にアップデートしてください。以下のパッケージを RHN(Red Hat Network)よりダウンロードし、インストール済みのパッケージに対して、適用してください。

・x86
net-snmp-5.3.2.2-9.el5_5.1.i386.rpm
net-snmp-devel-5.3.2.2-9.el5_5.1.i386.rpm
net-snmp-libs-5.3.2.2-9.el5_5.1.i386.rpm
net-snmp-perl-5.3.2.2-9.el5_5.1.i386.rpm
net-snmp-utils-5.3.2.2-9.el5_5.1.i386.rpm

・EM64T
net-snmp-5.3.2.2-9.el5_5.1.x86_64.rpm
net-snmp-devel-5.3.2.2-9.el5_5.1.i386.rpm
net-snmp-devel-5.3.2.2-9.el5_5.1.x86_64.rpm
net-snmp-libs-5.3.2.2-9.el5_5.1.i386.rpm
net-snmp-libs-5.3.2.2-9.el5_5.1.x86_64.rpm
net-snmp-perl-5.3.2.2-9.el5_5.1.x86_64.rpm
net-snmp-utils-5.3.2.2-9.el5_5.1.x86_64.rpm

参照：本修正に関する情報は、下記のエラータ情報も参照してください。
■エラータ情報 ：net-snmp bug fix update
http://rhn.redhat.com/errata/RHBA-2010-0422.html

ESMPRO/ServerAgent Ver. 4.5

6 よくある質問

ESMPRO/ServerAgent のよくある質問について説明します。

VMware ESX では、コンソールオペレーティングシステムが、仮想カーネル(VMkernel)にあるため、ESMPRO/ServerAgent for VMware は、ESMPRO/ServerAgent (Linux 版)と同等の機能を提供しています。

最新バージョンの ESMPRO/ServerAgent (Linux 版)は、次のウェブサイトからダウンロードできます。
予防保守の観点から最新バージョンの ESMPRO/ServerAgent (Linux 版)を、ご利用することをお勧めします。
https://www.express.nec.co.jp/linux/dload/esmpro/index.html
左側のメニューの「ESMPRO/ServerAgent」から「ソフトウェアのご使用条件」のご使用条件をご確認の上、「同意する」を選択します。
「ESMPRO/ServerAgent (Linux 版) ダウンロードページ」からご使用のディストリビューション(アーキテクチャー)を選択し、装置に合った物件を入手します。

最新バージョンの ESMPRO/ServerAgent for VMware は、次のウェブサイトからダウンロードできます。
■ESMPRO/ServerAgent for VMware サポート対象の追加物件
https://www.support.nec.co.jp/View.aspx?id=9010100940
※インストールには、ESMPRO/ServerAgent for VMware 製品メディアが必要です。

ESMPRO/ServerManagerから自動発見に失敗する

ファイアウォールの設定を確認する

ESMPRO/ServerManager から監視するとき、以下のポートを利用しています。お使いの環境でファイアウォールの設定をされているとき、以下のポートに対してアクセスを許可する設定か確認してください。

snmp 161/udp
snmp-trap 162/udp

snmpdが起動していることを確認する

以下のコマンドを実行して、snmpd が起動していることを確認してください。

ps ax | grep snmpd

- 起動しているときは、何もする必要はありません。
- 起動していないときは、snmpd の設定を変更した後、snmpd を起動します。

/sbin/chkconfig --level 35 snmpd on
/etc/init.d/snmpd start

portmap (またはrpcbind)が起動していることを確認する

以下のコマンドを実行して、portmap が起動していることを確認してください。

ps ax | grep portmap

- 起動しているときは、何もする必要はありません。
- 起動していないときは、portmap の設定を変更した後、portmap を起動し、サービスを再起動します。

/sbin/chkconfig --level 35 portmap on
/etc/init.d/ portmap start
/opt/nec/esmpro_sa/bin/ESMRestart

portmap の設定が表示されない場合は、rpcbind を使用している可能性があります。
portmap の設定を rpcbind に読みかえて確認してください。
※rpcbind を使用している OS：SUSE Linux Enterprise Server 11, Red Hat Enterprise Linux 6 など。

snmpdで使用するコミュニティー名の設定を確認する

snmpd.conf に設定したコミュニティー名と ESMPRO/ServerAgent で設定しているコミュニティー名が一致しているか確認してください。設定方法の詳細につきましては本書の 2 章(1. 全般プロパティ)を参照してください。

snmpd.confの内容を確認する

snmpd.conf に以下の設定があるか確認してください。

dlmod ntpass /opt/nec/esmpro_sa/lib/ntpass.so
ntpass .1.3.6.1.4.1.119.2.2.4.4
ntpass .1.3.6.1.2.1.10.7

上記の設定は ESMPRO/ServerAgent がインストール時に ESMPRO MIB と Ethernet Like MIB の SNMP 要求に対応するため、snmpd.conf に書き込む設定情報です。これらの設定が存在しないとき、上記の設定を追記後に snmpd を再起動してください。設定が存在しない原因は、ESMPRO/ServerAgent インストール後に snmpd の再インストールやアップグレードをしたことが考えられます。

登録済みの設定を確認する

オペレーションウィンドウに登録されているサーバー名、IP アドレスを確認してください。
オペレーションウィンドウに登録されているサーバーの「マシン名」または「IP アドレス」が登録しようとするサーバーの「マシン名」「IP アドレス」と重なっていないか確認してください。重なっていると登録できません。

/etc/hosts.deny、/etc/hosts.allowの内容を確認する

/etc/hosts.deny と/etc/hosts.allow ファイルの設定を確認してください。/etc/hosts.deny で原則禁止の設定をしているときは、/etc/hosts.allow ファイルで snmpd のアクセスの許可を設定してください。

本件に関する設定は、次のウェブサイトを参照してください。
Linux サービスセット : /etc/hosts.deny、/etc/hosts.allow を使ったアクセス制限(TCP wrappers)の方法を教えてください。【Linux サービスセットご契約のお客様限定】
https://www.support.nec.co.jp/View.aspx?id=3150005102

SELinux機能の設定状況を確認する

sestatus コマンドが存在しないとき、SELinux はインストールされていませんので、設定する必要はありません。

```
# sestatus -v
SELinux status: enabled        ←ここをチェックしてください。
        :
```

SELinux status: が enabled と表示されるとき、SELinux 機能が有効になっています。

- 有効のときは、snmpd サービスに対する SELinux のアクセス制限を変更してください。
  【Red Hat Enterprise Linux 6 のとき】
  ```
  # /usr/sbin/semanage permissive -a snmpd_t
  # /etc/init.d/snmpd restart
  ```
  【Red Hat Enterprise Linux 6 以外のとき】
  ```
  # setsebool -P snmpd_disable_trans 1
  # /etc/init.d/snmpd restart
  ```
- 無効のときは、snmpd サービスに対する SELinux のアクセス制限を変更する必要はありません。

ESMPRO/ServerManagerからの設定に失敗(しきい値の設定に失敗しました)。

snmpd.confの設定を確認する

ESMPRO/ServerManager から設定するとき、SNMP の書き込み権限が必要です。snmpd.conf の定義に write 権限が付与されているか確認してください。

記載例 1)

```
#       name            incl/excl    subtree        mask(optional)
view    all             included     .1             80

#       group           context sec.model sec.level prefix read   write   notif
access  notConfigGroup ""       any       noauth    exact  all    all     none
```

記載例 2)

```
#rocommunity public default
rwcommunity public default
```

ESMPRO関連のメッセージがsyslogへ記録され、OSの起動に時間が掛かります。

下記メッセージが表示される原因として考えられるのは、portmap(または rpcbind)が起動されていない可能性や ESMPRO/ServerAgent が使用するポートが開放されていない可能性が考えられます。

```
###ERR### Please check /opt/nec/esmpro_sa/work/ESMntserver.ready or fopen is failed(errno:2)
```

以下を確認してください。
・portmap(または rpcbind)が起動していることを確認してください。

・/etc/sysconfig/iptables の内容を確認してください。
システム内のプログラム間通信で使用されるループバック・インタフェースへの通信を許可する設定があるか確認してください。ファイアウォールを利用していないときは問題ありません。
例) -A INPUT -i lo -j ACCEPT

・/etc/hosts.deny と/etc/hosts.allow の内容を確認してください。
/etc/hosts.allow に対し、ループバックアドレスを許可する設定があるか確認してください。
例) ALL:localhost

コントロールパネル(ESMagntconf, ESMamsadm)に関する質問。

コントロールパネルが起動できない。

ディストリビューションやバージョンにより、必須パッケージは異なります。ESMPRO/ServerAgent 必須パッケージを確認していただき、ESMPRO/ServerAgent が動作に必要なパッケージがインストールされているか確認してください。ESMPRO/ServerAgent 必須パッケージは ESMPRO/ServerAgent ドキュメントに公開しています。

■ESMPRO/ServerAgent ドキュメント
http://www.express.nec.co.jp/linux/dload/esmpro/docs.html
必須パッケージ一覧 > ESMPRO/ServerAgent 必須パッケージ

VMware ESX では、ESMPRO/ServerAgent for VMware インストレーションガイドに記載している以下の手順を実行していないとき、本現象が発生します。以下の手順を実行し、OS を再起動します。

```
# cd /opt/nec/esmpro_sa/log/
# sh /(マウントポイント)/esmpro_sa/vmset.sh –sata
# reboot
```

コントロールパネルで日本語の表示、および入力ができない。

コントロールパネル(ESMagntconf、ESMpowersw)を日本語で表示させるためには、ネットワーク経由(ssh コマンドなど)で別の日本語端末からログインし、一時的に LANG 環境変数を日本語環境に変更してからコントロールパネルを起動してください。

コントロールパネルを起動するコンソールの LANG 環境変数を「ja_JP.eucJP」へ変更して、作業します。

```
# echo $LANG … 現在の LANG 環境変数を確認します。
# export LANG=ja_JP.eucJP
# cd /opt/nec/esmpro_sa/bin/
# ./ESMamsadm (または) ./ESMagntconf
```

作業終了後に元の LANG 環境変数へ変更します。
※LANG 環境変数は、OS に合わせ、ja_JP.eucJP や ja_JP.UTF-8 等を使用してください。

コントロールパネルで日本語の入力に切り替えできない。

ESMPRO/ServerAgent のコントロールパネルは、newt パッケージの機能を利用しています。newt パッケージのバージョンにより、切り替え方法が異なります。<Space>キーまたは<Ctrl>+<Space>キーを押して、入力の切り替えできるか確認してください。

ESMPRO/ServerAgent関連サービスに関する質問

ESMPRO/ServerAgent関連サービスを一括で停止や起動させたい。

root 権限のあるユーザーでログインし、ESMRestart コマンドを実行します。
【停止させるとき】
引数に"stop"を指定して、ESMRestart コマンドを実行します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart stop
```

【起動させるとき】
引数に"start"を指定して、ESMRestart コマンドを実行します。
/opt/nec/esmpro_sa/bin/ESMRestart start
【再起起動させるとき】
引数を指定せず、ESMRestart コマンドを実行します。
/opt/nec/esmpro_sa/bin/ESMRestart

snmpd の起動や停止はしません。

ESMPRO/ServerAgentの機能や仕様に関する情報を教えてください。

ESMPRO/ServerAgentが使用するポート番号を教えてください。

ESMPRO/ServerManager(以降、ESMPRO/SM と表記)から ESMPRO/ServerAgent(以降、ESMPRO/SA と表記)がインストールされた装置を監視するとき、以下のポートを利用しています。
お使いの環境でファイアウォールの設定をされるときは、これらへのアクセスを許可する設定にしてください。
表中「自動割当」の箇所は、OS により使用可能なポートを一定の範囲内で割り振られます。そのため固定することはできません。ポートの範囲は以下のファイルを参照してください。
/proc/sys/net/ipv4/ip_local_port_range

■ESMPRO/SA ←→ ESMPRO/SM

機能	ESMPRO/SA	方向	ESMPRO/SM	備考
自動登録 サーバー監視(SNMP)	161/udp	← →	161/udp	snmp
マネージャ通報(SNMP)	自動割当	→	162/udp	
マネージャ通報 (TCP/IP in Band, TCP/IP Out-of-Band)	自動割当	→ ←	31134/tcp	
マネージャ経由 エクスプレス通報サービス	自動割当	→ ←	31136/tcp	
HTTPS(マネージャ経由) エクスプレス通報サービス	自動割当	→ ←	31138/tcp	

※双方向のものは、上段の矢印が通信開始時のもので、下段は折り返しの通信を示します。
※マネージャ通報(TCP/IP)で使用するポート番号は、通報の設定画面より変更できます。

■ESMPRO/SA ←→ メールサーバー

機能	ESMPRO/SA	方向	メールサーバー	備考
エクスプレス通報サービス (インターネットメール)	自動割当	→ ←	25/tcp	smtp
		→ ←	110/tcp	pop3

※双方向のものは、上段の矢印が通信開始時のもので、下段は折り返しの通信を示します。
※エクスプレス通報サービス(インターネットメール)で使用するポート番号は、通報の設定画面より変更できます。

■ESMPRO/SA ←→ HTTPS サーバー

機能	ESMPRO/SA	方向	HTTPS サーバー	備考
エクスプレス通報サービス(HTTPS)	自動割当	→	443/tcp	https

ESMPRO/ServerAgent は以下の内部ポートを使用しています。
iptables を使ったパケットフィルタリング設定をするときは、これらへのアクセスを許可する設定にしてください。

■ESMPRO/SA ←→ ESMPRO/SA

機能	ポート番号
portmap(rpcbind)	111/tcp
	111/udp
ESMPRO/ServerAgent	自動割当

ESMPRO/ServerAgentの監視機能を教えてください。

ESMPRO/ServerAgent の監視機能は、ESMPRO/ServerAgent 監視項目一覧の機能概要を参照してください。
ESMPRO/ServerAgent 監視項目一覧は ESMPRO/ServerAgent ドキュメントに公開しています。

■ESMPRO/ServerAgent ドキュメント

http://www.express.nec.co.jp/linux/dload/esmpro/docs.html

監視項目一覧 ＞ESMPRO/ServerAgent 監視項目一覧

ESMPRO/ServerAgentのサービス(プロセス)の機能を教えてください。

ESMPRO/ServerAgent のサービス(プロセス)の機能は、ESMPRO/ServerAgent プロセス情報資料のプロセスの機能概要を参照してください。
ESMPRO/ServerAgent プロセス情報資料は ESMPRO/ServerAgent ドキュメントに公開しています。

■ESMPRO/ServerAgent ドキュメント

http://www.express.nec.co.jp/linux/dload/esmpro/docs.html

監視項目一覧 ＞ESMPRO/ServerAgent プロセス情報資料

ESMPRO/ServerAgentのWindows版とLinux版の機能差分を教えてください。

ESMPRO/ServerAgent (Linux 版)は、以下の機能が未サポートです。

・サーバ状態/構成情報でのディスクアレイ情報の表示

RAID 管理ユーティリティーを導入することにより、Syslog 監視機能を利用した通報機能のみサポートします。

■ESMPRO/ServerAgent ドキュメント

http://www.express.nec.co.jp/linux/dload/esmpro/docs.html

監視項目一覧 ＞ESMPRO/ServerAgent 監視項目一覧

■RAID コントローラの注意事項 - RAID 管理ユーティリティーの入手

http://www.express.nec.co.jp/linux/supported-help/note/notes1.html

RAID構成のストレージ監視はできますか？

ESMPRO/ServerAgent のストレージ監視機能はハードディスクドライブ単体構成のみのサポートであり、RAID 構成のストレージ監視はできません。RAID 構成のストレージ監視は、RAID 管理ユーティリティーを導入することにより Syslog 監視機能を利用した通報機能のみサポートします。

■RAID コントローラの注意事項 - RAID 管理ユーティリティについて

http://www.express.nec.co.jp/linux/supported-help/note/notes1.html

NICのLink Up/Downが通報されない。

ESMPRO/ServerAgent のネットワーク(LAN)監視はトラフィックを監視しているため、NIC の Link Up/Down は検出できません。カーネル、ドライバーなどにより、NIC の Link Up/Down 時に syslog(/var/log/messages)に記録されるメッセージがあるとき、Syslog イベントを追加することで通報できます。ただし、Link Down のときは、ネットワークが使用できない状態のため、通報されない可能性があります。

MIB定義ファイルは、どこに格納されていますか？

ESMPRO/ServerAgent が拡張している ESMPRO MIB(.1.3.6.1.4.1.119.2.2.4.4)の定義ファイルは、OS 種別(Windows、Linux、VMware 等)を問わず装置に添付されている EXPRESSBUILDER に格納しております。

【EXPRESSBUILDER Ver.5 以降】

(DVD):{レビジョンフォルダー}¥win¥ESMPRO¥JP¥MIBS

【EXPRESSBUILDER Ver.4】
(CD):¥ESMPRO¥MIBS または (CD):¥ESMPRO¥JP¥MIBS

{レビジョンフォルダー}は、EXPRESSBUILDER のバージョンにより異なります。
EXPRESSBUILDER Ver. 5.10-001.01 のとき、{レビジョンフォルダー}は 001 です。
また、以下の EXPRESSBUILDER では、複数の{レビジョンフォルダー}が存在します。
・EXPRESSBUILDER Ver. 5.40-001.03 以降
  001 : Express5800/120Bb-6, 120Bb-d6, 120Bb-m6
  002 : Express5800/B140a-T
・EXPRESSBUILDER Ver. 5.40-001.10 以降
  001 : Express5800/120Bb-6, 120Bb-d6, 120Bb-m6
  002 : Express5800/B140a-T
  003 : Express5800/B120a, B120a-d, B120b, B120b-d, B120b-Lw
・EXPRESSBUILDER Ver. 5.40-004.03 以降
  003 : Express5800/B120a, B120a-d, B120b, B120b-d, B120b-Lw
  004 : Express5800/B120b-h
・EXPRESSBUILDER Ver. 5.10-014.05 以降
  014 : Express5800/R110b-1, T110b
  019 : Express5800/R110c-1, T110c
・EXPRESSBUILDER Ver. 6.10-020.05 以降
  020 : Express5800/R110d-1E
  024 : Express5800/R110e-1E

ESMPRO/ServerAgentの通報に関する情報を教えてください。

ESMPRO/ServerAgentが通報するSNMPトラップ内容を教えてください。

ESMPRO/ServerAgent が通報する SNMP トラップ内容は ESMPRO/ServerAgent SNMP トラップ一覧を参照してください。ESMPRO/ServerAgent SNMP トラップ一覧は ESMPRO/ServerAgent ドキュメントに公開しています。

■ESMPRO/ServerAgent ドキュメント
http://www.express.nec.co.jp/linux/dload/esmpro/docs.html
SNMP トラップ一覧 ＞ESMPRO/ServerAgent SNMP トラップ一覧(Ver.4.5)/サービス監視
ESMPRO/ServerAgent SNMP トラップ一覧(Ver.4.5)/Syslog 監視

ESMPRO/ServerAgentが送信するSNMPトラップ内の文字コード

ESMPRO/ServerAgent が送信する SNMP トラップ内の日本語文字コードは、OS で使用している日本語文字コードに影響されず S-JIS に変換して送信しています。ESMPRO/ServerManager のアラートビューアは問題ありませんが、SNMP トラップを受信するソフトウェアの仕様によっては、S-JIS が表示できず文字化けする可能性があります。

ESMPRO/ServerManagerのアラートビューアで受信した通報が一部英語表記となる。ESMPRO/ServerAgentがsyslogに記録するメッセージが一部英語表記となる。

ESMPRO/ServerAgent 関連サービスは、各サービス起動時の LANG 環境変数の値を元に動作する言語(日本語と英語)を判断しております。Red Hat Enterprise Linux 5 以降では、OS の設定言語に関わらず、サービス起動時の LANG 環境変数は、英語環境(en_US.UTF-8)となります。通報内容を日本語で通知させるには、ESMPRO/ServerAgent 日本語設定ツール(esmset.sh)を実行することにより、ESMPRO/ServerAgent 関連サービスのみ、LANG 環境変数を日本語環境(ja_JP.UTF-8)で動作するように設定します。

ESMPRO/ServerAgent が送信する通報には、ESMPRO/ServerAgent 側から、すべてのメッセージを送信する Generic Trap と、ESMPRO/ServerAgent 側から、現在値等の可変値情報のみを送信して、ESMPRO/ServerManager 側で、メッセージを作成する predefine Trap があります。そのため、

ESMPRO/ServerManager のアラートビューアで受信するメッセージは日本語で表記される情報があります。

ESMPRO/ServerManagerのアラートビューアで受信した通報が「不明なサーバ」またはトラップの送信元と異なるサーバーが表示される。

＜ESMPRO/ServerManager の仕様＞
ESMPRO/ServerManager のアラートビューアは、ESMPRO/ServerAgent から送信された IP アドレス (AgentAddress フィールド)をオペレーションウィンドウに登録されているアイコンを順に検索し、IP アドレスと最初に合致するホスト名を表示します。アドレスは、インタフェースプロパティに登録されているアドレスも検索します。

＜ESMPRO/ServerAgent の仕様＞
/etc/hosts に自ホスト名が未設定のとき、ESMPRO/ServerAgent は UDP のソケット通信を利用して、TRAP 送信元の IP アドレスを取得します。

トラップの送信元 IP アドレスが 127.0.0.1 のときに、ESMPRO/ServerManager のオペレーションウィンドウに登録されている情報と一致したとき、トラップの送信元と異なるサーバーを表示するときがあります。また、登録されている情報と一致しなかったとき、「不明なサーバ」と表示します。

ESMPRO/ServerAgent の仕様にある gethostbyname()関数の取得データは、/etc/hosts の定義と関連付いていますが、/etc/host.conf の設定にも影響を受けるためすべての環境が以下と一致するとは限りません。上記 1) のホスト名が "server1" の場合は、/etc/hosts の内容によってどのような IP アドレスを取得するかの例を記載します。

(/etc/hosts の設定例 1) トラップの送信元 IP アドレス：127.0.0.1 となります。

```
127.0.0.1        server1  localhost.localdomain localhost
10.1.2.1         server1
10.1.2.2         server2
```

(/etc/hosts の設定例 2) トラップの送信元 IP アドレス：10.1.2.1 となります。

```
10.1.2.1         server1
127.0.0.1        server1 localhost.localdomain localhost
10.1.2.2         server2
```

(/etc/hosts の設定例 3) トラップの送信元 IP アドレス：10.1.2.1 となります。

```
127.0.0.1        localhost.localdomain localhost
10.1.2.1         server1
10.1.2.2         server2
```

ESMPRO/ServerAgentがsyslogに記録するメッセージを教えてください。

ESMPRO/ServerAgent が syslog に記録するメッセージは ESMPRO/ServerAgent SNMP トラップ一覧の通報メッセージを参照してください。

<例>

Sep 13 07:46:26 test-host ESMamvmain: SRC:ESMCommonService, ID:80000065, MSG:システムの温度が高くなっています。　センサ番号: 3　位置: フロントパネルボード 1　現在の温度: 42 度(C)　しきい値: 42 度(C)

上記メッセージと SNMP トラップ一覧の対応としては、以下のとおりです。

SRC:ESMCommonService　　= SNMP トラップ一覧の通報ソース名
ID:80000065　　= SNMP トラップ一覧の通報 ID
MSG:システムの温....　　= SNMP トラップ一覧の通報メッセージ

ESMPRO/ServerAgent SNMP トラップ一覧は ESMPRO/ServerAgent ドキュメントに公開しています。

■ESMPRO/ServerAgent ドキュメント
http://www.express.nec.co.jp/linux/dload/esmpro/docs.html
SNMP トラップ一覧 ＞ESMPRO/ServerAgent SNMP トラップ一覧(Ver.4.5)/サービス監視

ESMPRO/ServerAgentがsyslogに記録するメッセージのファシリティとプライオリティを教えてください。

ESMPRO/ServerAgent が syslog に記録するメッセージのファシリティとプライオリティはバージョンにより異なります。

【ESMPRO/ServerAgent Ver.4.2 以降】
情報　ファシリティ　：user
　　　プライオリティ：info
警告　ファシリティ　：user
　　　プライオリティ：warning
異常　ファシリティ　：user
　　　プライオリティ：err

【ESMPRO/ServerAgent Ver.4.1 以前】
情報　ファシリティ　：user
　　　プライオリティ：info
警告　ファシリティ　：user
　　　プライオリティ：info
異常　ファシリティ　：user
　　　プライオリティ：info

任意のメールアドレスへの通知やパトロールランプを鳴動させる方法を教えてください。

任意のメールアドレスへの通知やパトロールランプを鳴動させる方法はありません。
ESMPRO/ServerManager(Windows)をインストールしている管理 PC(Windows)に WebSAM AlertManager を導入することにより、運用環境に合わせた通報手段を提供しています。
【WebSAM AlertManager - 特長・機能の抜粋】
・システム管理者がどこからでも障害状況の確認ができる mail 通報
・サーバーの異常をサーバーのオペレーターに通知するポップアップ通報
・サーバーの異常情報をリモートプリンターにも印刷可能なプリンター書き出し
・サーバーの異常を検出した場合に、業務アプリケーションと連携して障害回避、障害復旧処理をする事を可能とするアプリケーションの実行
・サーバーの異常を検出した場合に、パトロールランプを鳴動させるパトロールランプ通報
・サーバーの異常情報履歴をファイル保存するファイル出力
■WebSAM AlertManager - 特長・機能
http://www.nec.co.jp/middle/WebSAM/products/p_am/kinou.html

ESMPRO/ServerAgentがサポートしているsnmpバージョンを教えてください。

ESMPRO/ServerAgent がサポートしている snmp バージョンは、SNMPv1 のみです。snmpd.conf の設定では、以下の波線が該当します。
【snmpd.conf の抜粋】

```
#       groupName          securityModel securityName
group   notConfigGroup v1               notConfigUser
group   notConfigGroup v2c              notConfigUser
```

ソース名やイベントIDを順番(昇順や降順)に表示する方法を教えてください。

ソース名やイベント ID の並び順は、カーネルのシステムコールである readdir()関数を利用しています。
readdir()関数からは、ファイル名順ではなく、inode 番号順に返却されるため、並び順を順番に表示できません。
※inode 番号 … ファイルシステムの管理情報の一つで識別番号(一意の番号)を指す。

設定を変更したときに再設定する必要がある項目を教えてください。

root権限のあるユーザーのパスワードを変更されるとき

・ESMPRO/ServerAgent 側の設定を変更する項目
　設定を変更する項目はありません。
・ESMPRO/ServerManager 側の設定を変更する項目
　設定を変更する項目はありません。

ESMPRO/ServerAgentマシン側のIPアドレスを変更されるとき

・ESMPRO/ServerAgent 側の設定を変更する項目
設定を変更する項目はありません。
・ESMPRO/ServerManager 側の設定を変更する項目
統合ビューア上に登録されている ESMPRO/ServerAgent アイコンの IP アドレスを変更してください。

ESMPRO/ServerAgentマシン側のコンピューター名(ホスト名)を変更されるとき

・ESMPRO/ServerAgent 側の設定を変更する項目
設定を変更する項目はありません。
・ESMPRO/ServerManager 側の設定を変更する項目
統合ビューアに登録されている ESMPRO/ServerAgent アイコンのホスト名を変更してください。統計情報自動収集を設定しているときは、ホスト名を変更すると、それまでの収集データを参照することができなくなります。
そのときは、
¥Program Files¥ESMPRO¥NVWORK¥esmpro 配下にある
元のホスト名.dat
元のホスト名.bak
というファイルのファイル名を、変更後のホスト名に合わせて変更してください。

ESMPRO/ServerManagerマシン側のIPアドレスを変更されるとき

・ESMPRO/ServerAgent 側の設定を変更する項目
マネージャ通報(SNMP/TCP_IP)に ESMPRO/ServerManager マシンの IP アドレスを指定しているときは、3 章の以下を参照して、コントロールパネル(ESMamsadm)から通報先の設定を変更してください。
2.1.1. マネージャ通報(SNMP)の基本設定
3.1.1. 通報手段がマネージャ通報(TCP_IP In-Band)の宛先設定
3.1.2. 通報手段がマネージャ通報(TCP_IP Out-of-Band)の宛先設定
また、snmpd に対して IP アドレスによるアクセスを制限しているときは、設定を変更してください。
/etc/snmp/snmpd.conf
/etc/hosts.allow
/etc/hosts.deny
・ESMPRO/ServerManager 側の設定を変更する項目
マネージャ間通信を使用しているときは、IP アドレスを変更した ESMPRO/ServerManager マシンとマネージャ間通信している相手側の ESMPRO/ServerManager マシン上の統合ビューアの設定を以下の手順で変更してください。
統合ビューアのメニュー
-> [オプション]
-> [カスタマイズ]
-> [マネージャ間通信]を選択します。
画面に設定されているESMPRO/ServerManagerのIPアドレスを新しいIPアドレスに変更してください。

ESMPRO/ServerManagerマシン側のコンピューター名(ホスト名)を変更されるとき

・ESMPRO/ServerAgent 側の設定を変更する項目
マネージャ通報(TCP_IP)に ESMPRO/ServerManager マシンのホスト名を指定しているときは、3 章の以下を参照して、コントロールパネル(ESMamsadm)から通報先の設定を変更してください。
3.1.1. 通報手段がマネージャ通報(TCP_IP In-Band)の宛先設定
3.1.2. 通報手段がマネージャ通報(TCP_IP Out-of-Band)の宛先設定
また、snmpd に対してホスト名によるアクセスを制限しているときは、設定を変更してください。
/etc/snmp/snmpd.conf
/etc/hosts.allow
/etc/hosts.deny

・ESMPRO/ServerManager 側の設定を変更する項目
設定を変更する項目はありません。

ドメインを変更されるとき

・ESMPRO/ServerAgent 側の設定を変更する項目
設定を変更する項目はありません。
・ESMPRO/ServerManager 側の設定を変更する項目
ESMPRO ユーザーグループをグローバルグループとして登録しているときは、ドメインを変更することでESMPRO ユーザーグループ へアクセスできない状態になると、ESMPRO/ServerManager が正常に動作しなくなりますので、ご注意ください。

MACアドレスを変更されるとき(ネットワークボードの交換など)

・ESMPRO/ServerAgent 側の設定を変更する項目
設定を変更する項目はありません。
・ESMPRO/ServerManager 側の設定を変更する項目
ESMPRO/ServerManager の Remote Wake Up 機能をご利用になられているとき、オペレーションウィンドウ上の対象サーバーのアイコンのプロパティ画面を開いて、[機能]タブの「RWU 機能 MAC アドレス」に新しい MAC アドレスを設定してください。

SNMPのコミュニティー名を変更されるとき

・ESMPRO/ServerAgent 側の設定を変更する手順
1) SNMP 設定ファイル(/etc/snmp/snmpd.conf)を編集して、コミュニティー名を変更する。
2) コントロールパネル(ESMagntconf)の「全般プロパティ」の「SNMP Community」にて、コミュニティー名を変更する。
3) snmpd サービスと ESMPRO/ServerAgent または OS を再起動する。

・ESMPRO/ServerManager Ver.5 Windows GUI の設定を変更する手順
1) サーバーの SNMP コミュニティー名に関する登録情報を変更する。
2) オペレーションウィンドウに登録しているサーバーアイコンのプロパティの SNMP コミュニティー(Get)と(Set)を変更する。
3) SNMP Service または OS を再起動する。

・ESMPRO/ServerManager Ver.5 WEBGUI 側の設定を変更する手順
1) サーバーの SNMP コミュニティー名に関する登録情報を変更する。
2) WEBGUI のサーバーの[サーバ設定]-[接続設定]-[変更]にて、SNMP コミュニティー名(取得用)と SNMP コミュニティー名(設定用)を変更する。
3) SNMP Service または OS を再起動する。